UNIVERSITÉ DE GRENOBLE

THÈSE

Pour obtenir le grade de

DOCTEUR DE L'UNIVERSITÉ DE GRENOBLE

Spécialité : **Sciences Juridiques – Droit Privé**

Arrêté ministériel : 7 août 2006

Présentée par

Mademoiselle Klervi RENAUDIN

Thèse dirigée par **Monsieur Jean-Michel BRUGUIÈRE**

préparée au sein du **Centre Universitaire d'Enseignement et de Recherche sur la Propriété Intellectuelle (CUERPI)**
dans **l'École Doctorale des Sciences Juridiques**

élaborée dans le cadre d'un contrat CIFRE, SELARL Iteanu, Avocats

Le *spamming* et le droit

Analyse critique et prospective de la protection juridique des « spammés »

Thèse soutenue publiquement le **11 juillet 2011**,
devant le jury composé de :

Madame Marie-Élodie ANCEL
Professeur à l'Université Paris-Est Créteil Val de Marne (Rapporteur)
Monsieur Jean FRAYSSINET
Professeur émérite de l'Université Paul Cézanne (Président et Rapporteur)
Monsieur David DECHENAUD
Professeur à l'Université Pierre Mendès France (Membre)
Madame Ségolène ROUILLE-MIRZA
Avocat au Barreau de Tours (Membre)

L'université de Grenoble n'entend donner aucune approbation ni improbation aux opinions émises dans les thèses ; ces opinions doivent être considérées comme propres à leurs auteurs.

À mon très cher oncle,

REMERCIEMENTS

Je tiens à remercier Monsieur le Professeur Jean-Michel BRUGUIERE pour avoir accepté de diriger mes travaux, pour ses conseils et pour m'avoir accordé sa confiance dans l'élaboration de cette étude.

Je tiens à remercier vivement Madame le Professeur Marie-Élodie ANCEL pour l'intérêt qu'elle a porté à mes travaux ainsi que pour ses conseils avisés qui m'ont permis d'approfondir mes recherches et d'orienter mes réflexions de manière constructive.

Je tiens également à adresser mes plus sincères remerciements à Sandrine et à Alix pour les remarques pertinentes dont elles ont toujours su faire preuve et qui m'ont permis de faire évoluer ce projet.

Je remercie également Charlotte, Ariane, Mélanie, Philippe, Delphine, Gersande et Élodie pour leur travail de relecture.

Enfin, ce travail n'aurait pu être achevé sans le soutien et les encouragements de ma famille et de mes amis.

Résumé

Rares sont les internautes qui peuvent encore affirmer ne jamais avoir reçu de *spams*, ces courriers électroniques non sollicités qui envahissent les boîtes aux lettres électroniques, jusqu'à, parfois, les saturer. À l'instar de tout échange de correspondance – sous forme papier ou numérique –, sa réception est subordonnée à la connaissance des coordonnées des futurs destinataires. Pour réaliser son opération, le « spammeur » doit donc nécessairement disposer de données nominatives telles que notamment, l'adresse électronique. Les enjeux économiques attachés à ces données à caractère personnel les exposent, de façon inévitable, à des risques accrus de collectes illicites. Engager une réflexion sur les moyens de protéger les « spammés » invite dès lors à raisonner à deux niveaux : lors de la collecte, pour empêcher la capture « sauvage » de telles données et lors de l'envoi proprement dit, afin de prémunir les destinataires contre la réception de ces messages indésirables. Face à des techniques anti-*spam* qui ont rapidement révélé leurs limites, la lutte contre le *spamming* s'est orientée vers l'outil législatif lequel sera également mis à rude épreuve. Au niveau national, les réponses offertes par les lois spéciales se révèlent incomplètes, voire inefficaces. Par ailleurs, la dimension intrinsèquement internationale du *spamming* ne permet pas d'ignorer les droits étrangers. En l'absence de consensus international, les profondes divergences entre législations nationales, en particulier entre la France et les États-Unis, premier pays émetteur de *spams,* risquent de compromettre leur effectivité à protéger les « spammés ». L'échec partiel des lois spéciales conduira ainsi à recourir aux solutions offertes par le droit commun en vue d'engager la responsabilité civile et pénale des « spammeurs ». Si d'un point de vue national, ces propositions démontreront leur capacité à pallier certaines insuffisances de la législation spéciale, la lutte anti-*spam* impliquera nécessairement d'engager une réflexion à l'échelle internationale.

Mots-clés

spamming – protection – données à caractère personnel – responsabilité – international

Abstract

Internet users who can still claim that they have never received spam are rare. These unexpected emails fill up, and sometimes blow up your mailbox. The reception of spam follows the same manner as other correspondence exchange, whether in paper or digital format. It is dependant on the knowledge of future recipients' contact information. In order to realize their operation, spammers must possess some private information, in particular email addresses. The economic issue attached to this private information puts them inevitably at increased risk of illegal collection. To think about the means of protection against spam invites us to reason at two levels : at the time of information collection to prevent illegal capture of private information and at the time of "sending" itself to protect recipients from receiving these undesirable messages. Antispam technology has quickly shown its limits. In light of this situation, the fight against spamming has turned towards legislative tools, which will be put to severe tests as well. At the national level, the answers provided by special laws seem to be incomplete, and even inefficient. In addition, the intrinsically international nature of spamming requires knowledge of foreign laws. Having no international consensus, the deep divergences between national legislations, in particular between France and United States, which is the first Spam-relaying country, risk jeopardizing their efficiency to protect spam victims. Thus, the partial failure of special laws leads us to seek recourse using the solutions provided by common law in preparation of engaging civil and criminal liability of spammers. If seen from a national point of view, the suggestions can demonstrate that they are capable of making up for some of insufficiency of special legislation, the antiSpam fight will necessarily involve a study at international scale.

Keywords

spamming – protection – personal data – responsability – international

Actu., actu.	Actualités juridiques
Actu. législ.	Actualité législative
ADV	*Advertisement*
AFA	Association française des Fournisseurs d'Accès et de Services Internet
Aff., aff.	Affaire
al.	Alinéa(s)
Alb. L. Rev.	*Albany Law Review*
Am.	*America, American*
amend.	*Amendment*
A. N.	Assemblée nationale
AOL	*AMERICA ONLINE Inc*.
APEC	*Asia-Pacific Economic Commission*
Apr.	*April*
Ariz. L. Rev.	*Arizona Law Review*
Art., art.	Article(s)
Ass. plén.	Assemblée plénière
Aug.	*August*
avr.	Avril
Berkeley Tech. L.J.	*Berkeley Technology Law Journal*
Bibl. dr. privé	Bibliothèque de droit privé
B.U. J. Sci. & Tech. L.	*Boston University Journal of Science & Technology Law*
Bull.	Bulletin
Bull. civ.	Bulletin des arrêts des chambres civiles de la Cour de cassation
Bull. crim.	Bulletin des arrêts de la chambre criminelle de la Cour de cassation
Bull. Joly	Bulletin Joly
c/	Contre
C.	Code
C. civ.	Code civil
C. com.	Code de commerce
C. Conso.	Code de la consommation
C. pén.	Code pénal
C. proc. civ.	Code de procédure civile
C. proc. pén.	Code de procédure pénale
Cal.	*California*
Cal.	*California Reports*
Cal.2d., Cal.Rptr. 2d	*California Reports Second Series, Second California Reports*
Cal.3d., Cal.Rptr. 3d [1]	*California Reports Third Series, Third California Reports*
Cal. Ct. App.	*Court of Appeal of California*
Cal. Rptr.	*California Reports*

[1] Trois États (California, New York et l'Illinois) ont leurs propres *Reporters* intitulés respectivement *West's California Reporter*, *West's New York Supplement* et *Illinois Decisions*.

Cal. L. Rev.	*California Law Review*
Cardozo Arts & Ent. L.J.	*Cardozo Arts & Entertainment Law Journal*
Cass.	Cassation
Cass. ass. plén.	Assemblée plénière de la Cour de cassation
Cass. civ. 1re	Première chambre civile de la Cour de cassation
Cass. civ. 2e	Deuxième chambre civile de la Cour de cassation
Cass. civ. 3e	Troisième chambre civile de la Cour de cassation
Cass. com.	Chambre commerciale de la Cour de cassation
Cass. crim.	Chambre criminelle de la Cour de cassation
Cass. req.	Chambre des requêtes de la Cour de cassation
C.D. Cal.	*U.S. District Court for the Central District of California*
C.F.R.	*Code of Federal Regulations*
CE	Conseil d'État
CEDH	Cour Européenne des Droits de l'Homme
Centr.	Central
ch.	Chambre
ch. crim.	Chambre criminelle
ch. corr.	Chambre correctionnelle
ch. instr.	Chambre de l'instruction
chap.	Chapitre
Chi-K. J. Intel. Prop.	*Chicago-Kent Journal of Intellectual Property*
chron.	Chronique
Cir.	*Circuit*
1st, 2nd, … Cir.	*The United States Court of Appeals for the 1st, 2nd, ….Circuit*
civ.	civil(e)
Civ. Act.	*Civil Action*
CJCE	Cour de Justice des Communautés Européennes
CNIL	Commission Nationale de l'Informatique et des Libertés
Co.	*Company*
coll.	Collection
Colum. J.L. & Soc. Probs.	*Columbia Journal of Law & Social Problems*
Colum.- VLA J.L. & Arts	*Columbia-VLA Journal of Law and the Arts*
comm.	Commentaire(s)
Comm. com. électr.	Communication Commerce Électronique
Comp., comp.	Comparez
Comp. L. Rev. & Tech. J.	*Computer Law Review & technology Journal Computer Law and Security Report*
Computer L.& Sec. Rep.	*Computer Law and Security Report*
cmt.	Comment(s)
concl.	conclusion(s)
Cons. const.	Conseil constitutionnel
Consid., consid.	Considérant
CNSA	*Contact Network of Spam Authorities*
Cont. conc. cons.	Contrats concurrence consommation

Cornell L. Rev.	*Cornell Law Review*
Corp.	*Corporation*
Corp. & Bus. L. J.	*Corporate and Business Law Journal (Australie)*
CPCE	Code des postes et des télécommunications
CPI	Code de la propriété intellectuelle
Ct.	Court
Ct. App.	*Court of Appeal*
D.	Décret
D.	Recueil Dalloz
DC	Décision
déc.	Décembre
DDHC	Déclaration des droits de l'homme et du citoyen
dern.	Dernier(s), dernières(s)
Dep.	*Department*
Dir., dir.	Directive
Doc. A.N.	Documentation de l'Assemblée nationale
Doc. fr.	La Documentation française
Doc. Sénat	Documentation du Sénat
doctr.	Doctrine
Dr., dr.	droit
Dr. et patr.	Droit et patrimoine
Dr. pénal	Droit pénal
Duke L.J.	*Duke Law Journal*
Duke L. & Tech. Rev.	*Duke Law & Technology Review*
éd.	Édition
Ed.	*Edition*
E.D.	*U.S. District Court for the Eastern District*
E.D. Mo.	*U.S. District Court for the Eastern District of Missouri*
E.D. Pa.	*U.S. District Court for the Eastern District of Pennsylvania*
E.D.Va.	*U.S. District Court for the Eastern District of Virginia*
ég.	Également
ENISA	*European Network and Information Security Agency*
esp.	Espèce
etc.	*Et cetera*
ex.	Exemple
Expertises	Expertises des systèmes d'information
F., F.2d, or F.3d	*Federal Reporter (1st serie, 2nd serie, …)*
F. Supp., F. Supp.2d	*Federal Supplement 1st serie, 2nd serie*
Fasc., fasc.	Fascicule
FCC	*Federal Communications Commission*
Feb.	*February*
févr.	Février
FTC	*Federal Trade Commission*
Gaz. Pal.	Gazette du Palais

gén.	Général
GLBA	*Gramm-Leach-Bliley Act*
H.R.	*House of Representatives*
Harv. L. Rev.	*Harvard Law Review*
I.R.	Information Rapide
Ibid., ibid., Ib., ib.	*Ibidem*
Id., id.	*Idem*
IFL	Loi informatique, fichiers et libertés
Inc.	*Incorporations/ed*
Ind. L. Rev.	*Indiana Law Review*
IUT	*International Telecommunication Union*
J. Broad. & Elec. Media	*Journal of Broadcasting and Electronic Media*
J.-Cl.	Juris-Classeur
J. High Tech. L.	*Journal of High Technology Law*
J. L . Econ. & Pol'y	*Journal of Law, Economics & Policy*
J. Legis.	*Journal of Legislation*
J. Marshall J. of Comp. & Info. L.	*The John Marshall Journal of Computer & Information Law*
J.O.	Journal officiel
J.O.U.E.	Journal officiel de l'Union européenne
J.O.U.E. n° C.	Série « Communications et informations » du Journal officiel de l'Union européenne qui contient les informations et avis concernant l'Union européenne (propositions de directives décision de la CJCE, notes, communiqués…)
J.O.U.E. n° L.	Série « Législation » du Journal officiel de l'Union européenne qui publie les textes qui entrent en vigueur (directives, règlements, décisions et recommandations)
J. Online L.	*Journal of Online Law*
J. Small & Emerging Bus. L.	*The Journal of Small & Emerging Business Law*
janv.	Janvier
JCP, éd. G	Juris-Classeur Périodique, édition générale
JCP, éd. E	Juris-Classeur Périodique, édition entreprises
JDI	*Journal du droit international (Clunet)*
juill.	Juillet
Juris-Data	Juris-Data (banque de données juridiques)
jurispr.	Jurisprudence
L. Ed.	*Lawyer's Edition*
L.G.D.J.	Librairie Générale de Droit et de Jurisprudence
L. Q. Rev.	*Law Quarterly Review*
LAP	*London Action Plan*
LCEN	Loi pour la Confiance dans l'Économie Numérique
LME	Loi de Modernisation de l'Économie
Loc. cit.	*Loco citato*
LPA	Les Petites Affiches
Ltd.	*Limited company*
Min. pub.	Ministère public

Mo.	*Missouri*
MoU	*Memorandum of Understanding* (Memorandum d'entente Séoul-Melbourne)
n.	*Note*
n°, n^{os}	Numéro, numéros
N.C.J.L. & Tech.	*North California Journal of Law & Technology*
N.D.	*U.S. District Court for the Northern District of*
N.D. Cal.	*U.S. District Court for the Northern District of California*
N.E.2d	*North Eastern Reporter Second*
N.W.2d	*North Western Reporter Second Series*
N.Y.U. L. Rev.	*New York University Law Review*
not.	Notamment
nov.	Novembre
NPRM	*Notice of Proposed Rulemaking*
NTIC, NTI	Nouvelles technologies de l'information et de la communication
obs.	Observation(s)
OCDE	Organisation de coopération et de développement économiques
oct.	Octobre, *October*
OMC	Organisation mondiale du commerce
ONU	Organisation des Nations Unies
op. cit.	*opere citato*
Or.	*Oregon, Oregon Supreme Court*
Or.	*Oregon Reports*
Or. App.	*Oregon Appellate Court Reports*
ord.	Ordonnance
ord. réf.	ordonnance de référé
P.	*Pacific Reporter*
P.2d.	*Pacific Reporter Second*
P.3d.	*Pacific Reporter Third*
p., pp.	Page, pages
P.U.A.M.	Presses Universitaires d'Aix-Marseille
P.U.F.	Presses Universitaires de France
P.U.L.	Presses universitaires de Lyon
Pa.	*Pennsylvania*
pan.	Panorama
prat.	Pratique
préc.	Précité/ée/és/ées
préf.	Préface
Propr. intell.	Propriété intellectuelle
Pub. L.	*Public Law*
Pub. Serv. Comm'n of N.Y	*Public Service Commission of the State of New York*
rapp.	Rapporteur
Rappr.	À rapprocher de
RCADI	Recueil des cours de l'Académie de droit international de La Haye

Rec.	Recueil
Rec. CJCE	Recueil des arrêts de la Cour de Justice des Communautés Européennes
Rec. const.	Recueil des décisions du conseil constitutionnel
RDC	Revue des contrats
RGDA	Revue générale du droit des assurances
Règl., règl.	Règlement
Répert.	Répertoire
Rép. Civ.	Répertoire de droit civil Dalloz
Répert. pénal	Répertoire de droit pénal Dalloz
Resp. civ. assur.	Responsabilité civile et assurances
Rev. crit. DIP	Revue critique de Droit International Privé
Rev. dr. publ.	Revue de droit public
Rev. sc. crim.	Revue de science criminelle et de droit pénal comparé
rev'd	*reversed*
Rich. J. L. & Tech.	*Richmond Journal of Law & Technology*
RIDC	Revue Internationale de Droit Comparé
RLDI	Revue Lamy Droit de l'Immatériel
Rptr.	*Report*
ROSKO	*Register of Known Spam Operations*
RRJ	Revue de la Recherche Juridique – Droit prospectif
RTD civ.	Revue Trimestrielle de Droit civil
RTD com.	Revue Trimestrielle de Droit commercial
RTD eur.	Revue Trimestrielle de Droit européen
s.	suivant/e/s/es
S.	Recueil Sirey
S. CT.	*Supreme Court Reporter*
S.D.	*U.S. District Court for the Southern District*
S.D. Ohio	*U.S. District Court for the Southern District oh Ohio*
S.D.N.Y.	*U.S. District Court for the Southern District of New York*
SACEM	Société des auteurs, compositeurs et éditeurs de musique
San Diego L. Rev.	*San Diego Law Review*
Santa Clara Computer & High Tech L.J.	*Santa Clara Computer & High Technology Law Journal*
SBL	*Spamhaus Block List*
SDRM	Société pour l'administration du droit de reproduction mécanique
Sec.	*Section*
sect.	Section
sept.	Septembre, *September*
spéc.	Spécialement
somm.	Sommaire commenté
sous la dir.	Sous la direction de
St. Mary's L.J.	*St Mary's Law Journal*
STAD	Système de traitement automatisé de données
Stat.	*Statute*

Sté	Société
T.	Tribunal
T. com.	Tribunal de commerce de
TA	Tribunal administratif
TGI	Tribunal de grande instance de
Trad., trad.	Traduction
Trav. Ass. H. Capitant	Travaux de l'Association Henri Capitant
Trav. Com. fr. DIP	Travaux du comité français de Droit International Privé
U. Chi. L. Rev.	*University of Chicago Law Review*
U. Dayton L. Rev.	*University of Dayton Law Review*
U. Rich. L. Rev.	*University of Richmond Law Review*
U.S.	*United State Reports*
U.S.	United States
U.S. Const.	*The United States Constitution*
U.S.C.	*United State Code*
U.S.F. L. Rev.	*University of San Francisco Law Review*
U.S.P.Q.2d.[2]	*United States Patents Quarterly Second.*
UCLA J.L. & Tech.	*University of California, Los Angeles Journal of Law & Technology*
UIT	Union Internationale des Télécommunications
UMKC L. Rev.	*University of Missouri-Kansas City Law Review*
v.	*versus*
V., v.	Voir, voyez
Va.	*Virginia, Supreme Court of Virginia*
Va. App.	*Virginia Appellate Court Reports*
Va. Code Ann.	*Annoted Code of Virginia*
Va. L. R.	*Virginia Law Review*
Vand. J. Ent. L. & Prac.	*Vanderbilt Journal of Entertainment Law & Pratice*
Vand. L. R.	*Vanderbilt Law Review*
vol.	volume
W.L.	*Westlaw*
Wash.	*Washington, Supreme Court of Washington*
Wash. U. L. Q.	*Washington University Law of Quaterly*
Wn.2d	*Washington Reports, 2nd Series*

[2] Un *reporter* spécial qui couvre les affaires relatives à la propriété intellectuelle : marques, brevets, *copyrights*, secrets de fabrication.

Afin de retrouver plus facilement les références des articles et décisions citées en droit américain, nous nous sommes permis d'adopter les usages utilisés en droit américain en matière de citation [3]. Il convient donc d'exposer brièvement les différents types de citations utilisés selon la source de la référence.

1- Les articles extraits de revues sont généralement cités de la façon suivante :

Patricia L. BELLIA, *Defending Cyberproperty*, 79 *N.Y.U. L. Rev.* 2164, 2260 (2004).
1 **2** **3** **4** **5** **6** **7**

1: Nom de l'auteur
2: Titre de l'article
3: Numéro du Volume (parfois l'année)
4: Nom de la revue
5: Numéro de la première page de l'article
6: Numéro de page visant un passage spécifique
7: Année de la publication (sauf si elle apparaît à la place du numéro de volume)

2- S'agissant des citations de jurisprudence, la méthode diffère selon que la juridiction saisie rélève du système fédéral ou des États.

- Au niveau de l'État fédéral :

Les affaires provenant de la Cour Suprême des États-Unis (*U.S. Supreme Court*) sont officiellement imprimées dans les *United States Reports* [4] et apparaissent sous la forme suivante :

John v. Smith, 346 *U.S.* 467 (1988).
1 **2** **3** **4** **5**

1: Nom de l'affaire
2: numéro du Volume du *reporter* dans lequel apparaît l'*opinion* de la cour
3: « US » pour *United State Reports*
4: numéro de la page dans le volume 346 du *United State Reports* où l'*opinion* commence
5: année à laquelle la cour a rendu sa décision

Les affaires provenant des cours d'appel intermédiaires du système judiciaire fédéral (*United States court of appeals* ou *Circuit Court*) sont publiées dans le *Federal Reporter* (*F.*, *F.2d*, or *F.3d*).

[3] Ces références sont basées sur deux ouvrages de référence en matière de citations juridiques, *The Bluebook : A Uniform System of Citation*, 18e Ed., 2005 et *The ALWD Citation Manual*, 2e Ed., 2003. L'ensemble des informations contenues dans ces deux ouvrages est disponible à l'adresse suivante : http://www.law.cornell.edu/citation/index.htm).

[4] Une même décision peut être publiée dans plusieurs *reporters* (*parallel citation*). Par exemple, outre le *United States Reports* pour les décisions de la *U.S. Supreme Court*, il existe plusieurs *reporters* non officiels : the *Supreme Court Reporter* (S. CT.), l'*United States Supreme Court Reports* et le *Lawyer's Edition* (*L. Ed.*). Par exemple, pour la citation « *John v. Smith*, 346 *U.S.* 467 (1988), 76 *S. CT.* 1145, 14 *L. Ed.* 2d 510 (1965) » : le "2d." signifie la seconde série du *Lawyer's Edition.*

Les affaires devant la *United States district court* sont publiées dans le *Federal Supplement* (*F. Supp*. or *F. Supp. 2d*). Les *judicial opinions* [5] sont les catégories de *legal material* les plus fréquemment cités. Lorsque les *lower federal court opinions* sont citées, la citation inclut le nom de la cour placé entre parenthèses immédiatement après l'année [6].

Lorsque l'affaire est disponible sous forme électronique mais pas encore sous un format imprimé, apparaissent : le nom de l'affaire, le n° du jugement (*docket number*), la source électronique, le numéro de la page précédé du symbole *, la cour et la date.

> Par exemple, *Hotmail Corp. v. Van$ Money Pie Inc.*, No. C-98 JW PVT ENE, C 98-20064 JW, 1998 WL 388389, at *7 (N.D. Cal. 1998).

- Au niveau des États :

Les décisions rendues par les cours d'État sont publiées différents *reports*. Beaucoup d'États ont leur propre *official state reporters* qui publient les décisions d'une ou plusieurs *state's courts.*

Les *reporters* qui publient les décisions d'un *state's highest court* ont le même nom abrégé que le nom de l'État : le *reporter* officiel des décisions de la *California Supreme Court* intitulé *California Reports* est abrégé en « Cal. » et pour les séries suivantes : « *Cal.2d* », « *Cal.3d* » ou « *Cal.4th* »).

> Par exemple : *Thrifty-Tel, Inc. v. Bezenek*, 54 *Cal. Rptr*. 2d 468, 473 (Ct. App. 1996) : il s'agit de l'affaire *Thrifty-Tel, Inc. v. Bezenek* devant la California Court of Appeal, 4th Apellate District, 3rd Division publiée dans le second *California Reports*, volume 54, page 468.

Outre les *official reporters*, plusieurs séries de *regional reporters* sont publiées, chacune couvrant plusieurs états. Il existe le *North Eastern Reporter,* l'*Atlantic Reporter,* le *South Eastern Reporter,* le *Southern Reporter,* le *South Western Reporter,* le *North Western Reporter,* and le *Pacific Reporter*. La Californie, l'Illinois et New York ont chacun leur propre *reporter,* en raison de l'important volume d'affaires générées dans ces États et intitulés respectivement : *West's California Reporter*, *Illinois Decisions*, and *West's New York Supplement*).

Voici quelques exemples de citation de jurisprudence :

> *Jackson v. Commonwealth*, 583 *S.E.2d* 780 (Va. Ct. App. 2003) :il s'agit d' une affaire jugée devant la cour d'appel de Virginie et publiée dans le *South Eastern Reporter*.

[5] L'*opinion* est un exposé des motifs dans une décision judiciaire.

[6] *Une district court* est formellement designee sous l'appelation suivante : " The United States District Court for…". (pour la décision référence sous la forme suivante : *Am. Online, Inc. v. Nat'l Health Care Disc., Inc*., 121 *F. Supp. 2d* 1255 (N.D. Iowa 2000), il convient de lire : « l'affaire *Am. Online, Inc. v. Nat'l Health Care Disc., Inc*., devant the *U.S. District Court for the Northern District of Iowa* publié dans le 2nd Federal Supplement, volume 121, page 1255).

Foxworth v. Maddox, 137 *So.* 161 (Fla. 1931) : il s'agit d'une affaire jugée devant la Cour suprême de Floride et publiée dans le *Southern Reporter*.

People v. Brown, 282 *N.Y.S.2d* 497 (1967) : une affaire devant la cour d'appel de New York publiée dans le *New York Supplement* et qui peut aussi apparaître dans le West's *regional reporter* sous la forme suivante : *People v. Brown*, 229 *N.E.2d* 192 (N.Y. 1967).

People v. Brown, 282 *N.Y.S.2d* 497 (1967)
1 2 3 4 5

1 : Nom de l'affaire
2 : numéro du volume du *reporter*
3 : *reported name*
4 : la première page où apparaît l'affaire dans ledit volume
5 : année

(Un plan détaillé de la thèse figure en fin d'ouvrage)

PREMIÈRE PARTIE : LES IMPERFECTIONS DE LA PROTECTION SPÉCIALE

TITRE PREMIER : LA MULTIPLICITÉ DES DÉFIS FACTUELS

CHAPITRE PREMIER : LE DÉFI TECHNOLOGIQUE

Section I. Un environnement technologique hostile
Section II. L'échec d'une réponse exclusivement technique

CHAPITRE SECOND : LES DÉFIS SOCIO-ÉCONOMIQUES

Section I. Les motivations économiques et justification du *spamming*
Section II. Une inquiétude sociale croissante

TITRE SECOND : LES LÉGISLATIONS SPÉCIALES FRAGILES

CHAPITRE PREMIER : DES LOIS DE PROTECTION DES DONNÉES INCOMPLÈTES FACE AUX MENACES DU *SPAMMNG*

Section I. En France, une protection uniforme à renforcer
Section II. Aux États-Unis, une protection contrastée à uniformiser

CHAPITRE SECOND : DES LOIS *ANTI-SPAM* PARTIELLEMENT INADAPTÉES AUX SPÉCIFICITÉS DU *SPAMMING*

Section préliminaire. Le choix entre deux réglementations des envois commerciaux, reflet d'une conception dualiste du *spamming*
Section I. En France, une prohibition de principe
Section II. Aux États-Unis, une autorisation de principe

SECONDE PARTIE : LE DÉPASSEMENT NÉCESSAIRE DE LA PROTECTION SPÉCIALE

TITRE PREMIER : LA RECHERCHE D'UNE ACTION EN RESPONSABILITÉ EFFICACE CONTRE LES « SPAMMEURS »

CHAPITRE PREMIER : L'ACTION EN RESPONSABILITÉ PÉNALE

Section I. Le *spamming*, une infraction autonome

Section II. Le *spamming*, vecteur de multiples infractions

CHAPITRE SECOND : L'ACTION EN RESPONSABILITÉ CIVILE

Section I. Le *spamming*, générateur de responsabilité délictuelle

Section II. Le *spamming*, générateur de responsabilité contractuelle

TITRE SECOND : L'ABANDON NÉCESSAIRE D'UNE LOGIQUE NATIONALE : LES MÉRITES DU DROIT INTERNATIONAL PRIVÉ

CHAPITRE PREMIER : LES JUSTIFICATIONS DU RECOURS AU DROIT INTERNATIONAL PRIVÉ

Section I. Un fléau sans frontières : L'internationnalité du *spamming*

Section II. À la recherche d'une réponse juridique globale

CHAPITRE SECOND : LES APPLICATIONS DU DROIT INTERNATIONAL PRIVÉ EN MATIÈRE DE *SPAMMING*

Section préliminaire. La question de la qualification en matière de *spamming*

Section I. Les conflits de juridictions suscités par le *spamming*

Section II. Les conflits de lois occasionnés par le *spamming*

INTRODUCTION GÉNÉRALE

Have you got anything without spam?"

"Well, there's spam egg sausage and spam, that's not got much spam in it."

"I don't want ANY spam!"

Monty Python's Flying Circus, " Spam ", Season 2, Episode n° 25 (1970) [7].

1. Origine du terme « *spam* ». Le terme *spam* a été inventé en 1937 à l'issue d'un concours organisé par la société américaine HORMEL FOODS qui offrait la possibilité de gagner la somme de 100 dollars à la personne dont le nom qu'elle proposerait serait retenu pour désigner du jambon épicé, leur nouveau produit. C'est ainsi que le mot « SPAM » a été choisi pour devenir la marque de jambon froid insipide qui accompagnait les soldats américains lors de la deuxième guerre mondiale et qui n'est autre que l'acronyme de « *Spiced Pork and Meat* » [8]. Le terme « *spam* », tel qu'on le connaît aujourd'hui, est apparu au cours des années 1980 suite à un incident survenu au sein de la Communauté MUD (*Multi-User Domain* ou *Multi-User Dungeon*) qui regroupe les passionnés de jeux de rôle en ligne et, au cours duquel, un utilisateur avait créé un macro [9] qui répétait, à de nombreuses reprises, le terme « *spam* » et avait occasionné de sévères dysfonctionnements techniques [10]. Il semblerait que le plaisantin ait été inspiré par un sketch mis en scène dans les années 70 par le célèbre groupe d'humoristes anglais les *Monty Python*, dans un des épisodes de la série télévisée, *Monty Python's Flying Circus*. La scène se déroulait dans un restaurant où la serveuse présentait le menu dans lequel chaque plat contenait du *spam :* " *egg and spam; egg bacon and spam; egg bacon sausage and spam; spam bacon sausage and spam; spam egg spam spam bacon and spam; spam sausage spam spam bacon spam tomato and spam* ". Pour parodier l'omniprésence de cet aliment, les comédiens se sont mis à scander le terme *spam* de façon si répétitive et si forte qu'ils couvraient la voix des autres protagonistes [11].

[7] Pour visualiser le sketch, consultez l'adresse suivante : http://www.youtube.com/watch?v=anwy2MPT5RE.
[8] V. par ex. *Verizon Online Services, Inc. v. Ralsky*, 203 *F. Supp.2d* 601, spéc. 606 (E.D.Va., June 7, 2002) (" *SPAM ® (Spiced Pork and Ham) in upper case letters is the registered trademark of Hormel Foods* ").
[9] Il s'agit d'une commande que le joueur programme pour qu'elle effectue une action de façon automatique lorsqu'il appuie sur celle-ci.
[10] V. David E. SORKIN, *Technical and Legal Approaches to Unsolicited Electronic Mail*, 35 *U.S.F. L. Rev.* 325, spéc. p. 325, note 2 (2001).
[11] V. *Verizon Online Services, Inc. v. Ralsky*, aff. préc., spéc. 606 (" *The term " spam " in lower case letters, and used in connection with [Unsolicited Bulk E-mail], derives from the sketch by the British comedy troupe Monty Python, in which a group of Vikings chant the word spam in a café whose breakfast menu is devoid of all else* ",

2. Première apparition d'un cas de *spamming*. Contrairement à une idée généralement reçue, la pratique du *spamming* [12] est apparue avant l'avènement de l'internet. Il a en effet, été émis pour la première fois sur le réseau ARPANET (*Advanced Research Projects Agency Network*), premier réseau de communication créé en 1969 par les services militaires américains. Le 3 mai 1978, Gary THUERK, un responsable *marketing* de la société informatique DIGITAL EQUIPMENT CORPORATION, avait envoyé sans mauvaise intention un message publicitaire vantant les mérites de nouveaux produits informatiques à presque 400 personnes de la côte ouest des États-Unis, suscitant le mécontentement général des destinataires [13]. Le premier cas de *spamming* était donc né mais rien ne laissait présager à cette époque que cette pratique, qui consiste à envoyer de très nombreux messages simultanément, deviendrait une véritable « plaie du *Web* ».

3. Des envois abusifs à des fins non commerciales. Par analogie au sketch des *Monty Python*, l'expression *spam* a été reprise dans les années 90 pour désigner, sur les groupes de discussion (*newsgroups*) sur *Usenet* [14], des articles postés qui n'avaient aucune pertinence au regard du thème de la discussion et qui violaient la politique du forum et les règles d'usage en la matière.

4. Des envois abusifs à des fins commerciales. Coïncidant avec l'utilisation croissante de l'internet comme moyen de prospection commerciale, l'histoire du *spamming* à grande échelle a débuté aux États-Unis en 1994, lorsqu'un couple d'avocats de l'Arizona, Lawrence CANTER et Martha SIEGEL qui, cherchant à attirer de nouveaux clients, proposaient de fournir une prestation de conseil à tous les candidats qui souhaitaient obtenir un visa américain [15]. Le message publicitaire vantait ainsi les services du cabinet en matière d'obtention d'une *Green Card*, une carte de travail étasunienne contre le versement de 100 dollars. Le même message avait été posté sur plus de 6.000 groupes de discussion, soit environ 10% du trafic quotidien sur *Usenet* à l'époque. En retour, plusieurs dizaines de milliers de destinataires avaient bombardé de messages de contestation l'adresse électronique

citant : Monty Python's Flying Circus, Just The Words, Vol. II, spéc. 27-29 (Methun, London 1989)). – *CompuServe, Inc. v. Cyber Promotions, Inc.*, 962 *F. Supp*. 1015, spéc. 1018, n.1 (S.D. Ohio, Feb. 3,1997).

[12] Les termes « *spamming* » et « spam » sont des termes anglais. Toutefois, en raison de leur utilisation courante dans le langage français, nous nous sommes permis de les naturaliser et de les utiliser tels quels dans l'ensemble de cette thèse. Le *spamming* désignant ainsi la pratique qui consiste à envoyer des messages, les *spams*. Concernant les termes « spammeur » et « spammé », il s'agit de néologismes dérivés du terme « *spamming* » que nous nous sommes autorisés à franciser pour la clarté de notre exposé : le « spammeur » désignant l'expéditeur de *spams*, le « spammé » désignant, pour sa part, le destinataire de *spam* et plus largement, tout personne touchée directement ou indirectement par une opération de *spamming*.

[13] Pour visualiser le message qui avait été envoyé, v. AROBASE, « Le spam a 30 ans ! », disponible sur: http://www.arobase.org/culture/premier-spam.htm.

[14] V. glossaire.

[15] Sur l'histoire du *spamming*, v. not. Alan SCHWARTZ et Simson GARFINKEL, *Stopping Spam*, 1re éd., O'Reilly, 1998, spéc. pp. 17-35.

du couple, provoquant une surcharge de leur serveur leur permettant d'accéder au réseau [16]. Le résultat de cette opération fut toutefois particulièrement lucratif puisque le revenu directement imputable à ces envois avaient été évalué à 200.000 dollars pour un coût de revient dérisoire. Au regard de son ampleur, cette opération marqua ainsi un véritable tournant dans l'évolution de la pratique du *spamming* et fut considérée comme le premier cas de publipostage (*mailing*) à grande échelle, désignée par l'expression « *Green Card Spam* ». Progressivement, ce phénomène s'est étendu aux services de courrier électronique [17] pour le plus grand inconfort de milliers d'internautes. Le terme *spam* est alors utilisé pour désigner les *e-mails* de rebut (*junk mail*), généralement pour des publicités de produits et services douteux.

5. La recrudescence du *spamming*. En juillet 1995, Jeff SLATON, surnommé le « Roi du *spam* » (*Spam King*), fut surtout célèbre pour avoir amélioré la pratique du *spamming* en créant la fausse adresse électronique et le faux nom de domaine afin de ne pas être identifié et éviter les déconvenues qu'avait connues le couple CANTER et SIEGEL. Dans les années 90, Sandford WALLACE créa la société CYBER PROMOTIONS. Déjà réputé dans le milieu du *marketing* pour l'envoi massif de télécopies non sollicitées, il est devenu en 1996 l'un des « spammeurs » les plus prolifiques des États-Unis, lui valant ainsi le surnom de « S*pamford* ». À partir de cette date, il mit pour la première fois à disposition du public son propre accès à l'internet et son nom de domaine pour diffuser des *spams*. Cette initiative lui permit ainsi, par l'intermédiaire d'un *spamware* [18] qu'il avait créé, de collecter plus d'un million d'adresses du célèbre fournisseur d'accès internet (ci-après FAI), AOL, et de leur envoyer des messages. Chaque abonné d'AOL présent sur sa liste recevait ainsi entre deux et cinq *spams* par jour. Au plus fort de son activité, il ressort que la société CYBER PROMOTION pouvait expédier jusqu'à 30 millions de *spams* par jour. En signe de riposte, AOL développa un système de défense destiné à bloquer systématiquement tous les messages en provenance de cette société. En 1997, cette dernière créa son propre nom de domaine < spamford.com > mais rencontra de plus en plus de difficultés à trouver un fournisseur consentant à l'envoi de *spams*. Par la suite, l'essor du *spamming* continua et atteint son apogée lors des attentats qui frappèrent les États-Unis le 11 septembre 2001. À compter de cette catastrophe, des rumeurs circulaient quant à une possible contamination par l'anthrax par voie postale, rumeurs qui

[16] V. par ex. Wye-Keen KHONG, " Regulating Spams on the Internet ", *in Electronic Datasets and Access to Legal Information*, conférence du 14 avril 2000, spéc. p. 4 (disponible sur : http://www.bileta.ac.uk/00papers/khong.html).)

[17] Depuis la parution du Journal Officiel du 20 juin 2003, le terme « courriel » a été adopté comme terminologie principale du courrier électronique dans la langue française. Toutefois, le terme « courrier électronique » et son équivalent anglais « *e-mail* », étant les plus usités dans le langage courant, nous nous autoriserons à utiliser indifféremment l'un de ces trois termes.

[18] V. glossaire.

engendrèrent un fort ralentissement de la prospection commerciale traditionnelle par papier, les destinataires n'osant plus ouvrir leur correspondance. Les annonceurs furent alors contraints de repenser leur méthode de prospection en privilégiant notamment les envois commerciaux par voie électronique afin de s'assurer du succès de leurs opérations promotionnelles de fin d'année. Mais ce ne fut que deux ans plus tard, à l'occasion d'une réflexion initiée par l'INTERNET ENGINEERING TASK FORCE (IETF) sur les technologies anti-*spam*, que le *spamming* fut reconnu officiellement comme une véritable menace qu'il convenait de ne plus ignorer.

6. Profil des « spammeurs ». On pourrait imaginer que seul un groupe restreint de « spammeurs », particulièrement doué et muni de solides connaissances techniques, pourrait être capable de contourner les filtres anti-*spam* et de bombarder les boîtes électroniques des utilisateurs. La réalité est néanmoins toute autre. Bien qu'une forte majorité de *spamming* soit orchestrée par des « spammeurs » professionnels comme le révèle la liste ROSKO qui répertorie les dix « spammeurs » les plus dangereux [19], il semble toutefois que le coût de revient tout à fait négligeable du *spamming* permette aisément à quiconque ayant un minimum de connaissances techniques de devenir « spammeur » [20]. Pour entreprendre une opération de *spamming*, il est simplement requis un coût initial de lancement correspondant à un ordinateur basique, un logiciel de collecte d'adresses qui coûte en moyenne 50 dollars, ou un fichier d'adresses déjà créé (un million d'adresses coûte entre 20 et 100 dollars) [21], ainsi qu'une connexion Internet haut débit. Il est donc avantageux pour les annonceurs de recourir à cette pratique en raison d'un coût d'émission très faible. Par ailleurs, le *spam* mobile, c'est-à-dire l'envoi de messages indésirables sur les téléphones portables, est également une technique très lucrative pour les « spammeurs ». Il peut se manifester par un appel direct ou sous la forme de SMS [22] ou de MMS [23] dont le but est d'éveiller la curiosité des personnes contactées et les conduire à rappeler un numéro qui est surtaxé [24]. Le caractère très lucratif de cette pratique provient du fait que la création d'un numéro surtaxé est gratuite et très simple. De très nombreux sites Internet proposent d'ouvrir

[19] V. THE SPAMHAUS PROJECT, " The 10 Worst Spammers" , 6 mai 2011, disponible sur : http://www.spamhaus.org/statistics/spammers.lasso. – Sur cette liste, v. *infra* ; n° 115.
[20] Bill HUSTED & Ann HARDIE, " Spam Wars Play Out Across Internet", *The Atlanta Journal-Constitution*, 14 déc. 2003, disponible sur : http://www.tomandmaria.com/110/Readings/Religious%20Spammer%20article.pdf.
[21] v. Yuri NAMESTNIKOV, " The economics of botnet ", 2009, disponible sur : http://www.securelist.com/en/downloads/pdf/ynam_botnets_0907_en.pdf. – V. ég. CNIL, *Rapport d'activité 1999*, n° 20, Doc. fr., 2000 spéc, p. 107 (qui faisait déjà le constat en 1999 qu il était « *possible de se procurer sur internet pour des sommes modiques des CD-ROM contenant 60 millions d'adresses électroniques (620 francs pour 2 millions d'adresses électroniques*).
[22] V. glossaire.
[23] V. glossaire.
[24] Ces messages sont du type : « Salut, c'est moi ! rappelle moi vite au 08. » ou « vous êtes le grand gagnant d'une loterie, pour découvrir votre lot, appelez au plus vite le 08… ».

des lignes surtaxées. Pour paramétrer ce type de ligne commençant par le numéro « 08 », il suffit de compléter un formulaire d'inscription en ligne et, en quelques minutes, le numéro étant créé, qu'il soit vérifié que l'activité réellement menée soit conforme à celle initialement déclarée lors de l'enregistrement. À chaque appel reçu facturé, le titulaire du numéro surtaxé reversera une partie – environ, les deux tiers – à l'entreprise qui propose le service d'appel surtaxé. Une fois le numéro d'appel créé, il reste toutefois à préciser comment s'opère la récupération des numéros à contacter. Cette opération est elle aussi très simple. Il suffit de créer une pondeuse d'appels, un système informatique permettant d'envoyer simultanément un appel, un SMS ou un MMS à un très grand nombre de téléphones portables. Le processus de création est encore une fois très accessible pour la plupart internaute puisqu'il leur suffit de récupérer des programmes informatiques gratuits disponibles sur l'internet. Les logiciels téléchargés permettent de générer presque instantanément une liste aléatoire de numéros de téléphone. Peuvent ainsi être créés 4.000 numéros en quelques secondes. Une fois la liste de numéros constituée, un programme informatique très simple permet de contacter, de façon synchronisée, tous les numéros répertoriés. La pondeuse ne coûte rien à son utilisateur puisque tous les appels passent par l'internet.

7. Une technique de prospection unique. Pour décrire la pratique du *spamming*, certains l'ont présenté comme aussi élémentaire que celle qui consiste à glisser des brochures dans les boîtes aux lettres ou sous les essuie-glaces des véhicules en stationnement [25]. Toutefois, ces deux techniques se distinguent à plusieurs égards. Tout d'abord, d'un point de vue fonctionnel, alors que la diffusion de *spams* ne sera rendue effective que si le « spammeur » dispose d'informations identifiantes, en particulier d'adresses électroniques, la distribution de publicités dans nos boîtes aux lettres ou sur nos pare-brises n'est pas subordonnée à la collecte préalable de ce type de données. Ensuite, la spécificité du *spamming* se manifeste par son ampleur. Des études récentes révèlent que cette pratique représente environ 85% de l'ensemble des *e-mails* échangés dans le monde [26]. L'un des employés de SYMANTEC rapporte qu'en 2010, le nombre de *spams* envoyés chaque jour par *e-mail* est estimé entre 100 et 200 milliards [27]. Les « spammeurs » utilisent généralement

[25] Serge GAUTHRONET et Étienne DROUARD, *Communications commerciales non sollicités et données personnelles* (Internal Market DG – Contract n° ETD/99/B5-3000/E/96), janv. 2001, spéc. p. 14, disponible sur : http://www.rigacci.org/docs/biblio/online/spam_garante/document/434683.pdf.

[26] Selon le rapport de novembre 2010 de la société SYMANTEC, spécialisée dans la création de solutions destinées à assurer la sécurité et l'intégrité des données, le *spamming* a représenté 86,61% de l'ensemble des *e-mails* échangés dans le monde en octobre 2010 et 89,4% en septembre 2010 (" State of Spam and Phishing ", n° 47, nov. 2010, disponible sur : http://www.symantec.com/content/en/us/enterprise/other_resources/b-state_of_spam_and_phishing_report_11-2010.en-us.pdf).

[27] Daren LEWIS, " The recent drop in global spam volumes – what happened ", 6 octobre 2010, disponible sur : http://www.symantec.com/connect/blogs/recent-drop-global-spam-volumes-what-happened.

des messages de petite taille (inférieur à 5Kb) qui peuvent être rapidement expédiés et en grande quantité [28]. Enfin, la particularité du *spamming* résulte du changement d'échelle des risques qui en découlent : les coûts financiers qui peuvent notamment en résulter apparaissent en effet sans commune mesure avec la gêne que suscitent les publicités « classiques » reçues quotidiennement dans nos boîtes aux lettres. À ces risques s'ajoutent les menaces qui pèsent sur les données nominatives, en particulier les adresses électroniques, puisqu'elles sont le plus souvent collectées à l'insu de leur titulaire. Face à l'ensemble de ces effets dommageables, engager une réflexion destinée à rechercher une protection juridique efficace des « spammés » apparaît donc essentielle.

8. Les raisons de l'essor du *spamming*. À la différence des moyens de sollicitations traditionnels (par papier ou *via* des appels téléphoniques), le *spamming* constitue une technique de prospection particulièrement efficace puisqu'il permet de transmettre un message, de façon presque instantanée, à des milliers voire des millions de personnes. Par ailleurs, son caractère très lucratif lui permet de remporter un vif succès. Il n'existe en effet aucun rapport de proportionnalité entre le nombre d'envois et le coût de revient : le coût d'envoi des *spams* est quasi nul pour les « spammeurs » puisqu'il est directement répercuté sur les FAI et les destinataires (*cost-shifting*) [29]. Les prix de *spam* varient selon le public ciblé et le nombre d'adresses ciblées. Le prix d'un postage ciblé peut s'étendre de 70 dollars pour quelques milliers d'adresses à 1.000 dollars pour des dizaines de millions. En 2008, les « spammeurs » ont engrangé un résultat impressionnant qui d'élève à environ 780.000.000 dollars grâce à l'envoi de *spams* [30]. Une liste d'un million d'adresses électroniques coûte en général entre 20 dollars et 100 dollars au « spammeur ». L'envoi de *spams* vers cette liste lui permettra ensuite d'engranger un profit pouvant s'élever à 150, voire 200 dollars [31]. En outre, le faible prix de l'accès à l'internet et l'augmentation de l'espace de stockage d'*e-mails* disponible gratuitement lui permettent d'atteindre des millions de destinataires pour un coût dérisoire. Ce coût tend encore à s'alléger puisque le « spammeur » est exempté des frais liés à l'impression et à l'affranchissement des messages comme il est de coutume pour les envois postaux et n'a pas besoin de mobiliser un personnel important tel que nécessaire pour les activités télémarketing (*marketing* par téléphone).

[28] SYMANTEC; " State of Spam and Phishing ", rapport 2010 préc.
[29] Pour plus de précisions, v. OCDE, *Les logiciels malveillants (maliciels) : Une menace à la sécurité de l'économie de l'Internet*, DSTI/ICCP/REG(2007)5/FINAL, 27 mai 2008, spéc. pp. 34-35, disponible sur : http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP/REG%282007%295/FINAL&docLanguage=Fr. – V. ég. David E. SORKIN, "Technical and Legal Approaches to Unsolicited Electronic Mail ", art. préc.
[30] v. Yuri NAMESTNIKOV, " The economics of botnet ", 2009, disponible sur : http://www.securelist.com/en/downloads/pdf/ynam_botnets_0907_en.pdf.
[31] v. Yuri NAMESTNIKOV, " The economics of botnet ", 2009, disponible sur : http://www.securelist.com/en/downloads/pdf/ynam_botnets_0907_en.pdf.

Enfin, l'accès de plus en plus facile à des techniques de collecte d'adresses électroniques et le recours à des ordinateurs compromis (réseaux *zombies*), facilement accessibles, favorisent la propagation de *spams* tout en réduisant toujours davantage les coûts d'émission.

9. Après cette brève présentation du *spamming*, il convient à présent de s'interroger sur les raisons qui nous ont conduits à faire le choix d'axer notre étude sur « le *spamming* et le droit ». Trois questions très simples peuvent synthétiser le fil conducteur de notre recherche : Quoi ?, Pourquoi ?, Comment ?. Pour répondre à chacune de ces interrogations, il conviendra tout d'abord de délimiter l'objet de la recherche (§. I.) puis, de préciser l'intérêt de cette dernière (§. II.) et enfin, d'exposer la méthode adoptée ayant guidé l'ensemble de nos travaux (§. III.).

§ 1. L'OBJET DE LA RECHERCHE

10. La première étape à laquelle est confronté quiconque envisage d'engager une réflexion sur un objet de droit est le traditionnel et incontournable exercice de définition. Nécessaire, cette étape permet de cadrer l'objet de notre étude et de définir précisément les éléments qui feront l'objet des réflexions à venir. Après avoir défini ce qu'il faut entendre par le terme « *spamming* » (A.) ; il conviendra d'identifier les droits qui seront sollicités au cours de notre étude (B.).

A. LE *SPAMMING*

11. La recherche d'une définition objective. Sans définir clairement le *spamming*, l'article 22 de la loi pour la confiance dans l'économie numérique, dite LCEN [32] rattache la réglementation de cette pratique à celle des envois commerciaux. L'article 22 de cette loi dispose qu'« [e]*st interdite la prospection directe au moyen d'un automate d'appel, d'un télécopieur ou d'un courrier électronique utilisant, sous quelque forme que se soit, les coordonnées d'une personne physique qui n'a pas exprimé son consentement préalable à recevoir des prospections directes par ce moyen* ». Plus précise, la Commission nationale de l'informatique et des libertés (CNIL) a initialement décrit cette pratique comme : « *l'envoi massif – et parfois répété – de courriers électroniques non sollicités, le plus souvent à*

[32] Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, J.O. n° 143 du 22 juin 2004, p. 1168 et s.

caractère commercial, à des personnes avec lesquelles l'expéditeur n'a jamais eu de contact et dont il a capté l'adresse électronique dans les espaces publics de l'internet : forums de discussion, listes de diffusion, annuaires, sites web, etc. » [33]. La Commission a, par la suite, complété cette définition en visant l'opération préalable à l'envoi de *spams*¸ à savoir la collecte d'adresses électroniques. Elle a ainsi précisé que le *spamming* procédait en amont d'une collecte irrégulière, irrégularité déduite de la violation des principes directeurs et des obligations en la matière et fixés par la loi du 6 août 2004 [34], dite loi « informatique, fichiers et libertés », encore désignée sous son acronyme « loi IFL » : « [c]*onstituent des " spams " les messages adressés sur la base d'une collecte irrégulière de méls* [sic], *soit au moyen de moteurs de recherche dans les espaces publics de l'internet (sites web, forums de discussion, listes de diffusion, chat…), soit que les adresses aient été cédées sans que les personnes n'en aient été informées et sans qu'elles aient été mises en mesure de s'y opposer ou d'y consentir. Une telle collecte est alors déloyale et illicite au sens de l'article 25 de la loi du 6 janvier 1978* » [35]. La jurisprudence française a également consacré une première définition juridique *a minima* du *spamming*, à savoir : « *l'envoi de messages non sollicités* » [36].

12. Si la CNIL a le mérite de proposer une définition relativement aboutie de ce phénomène, nous verrons que les critères retenus ne peuvent toutefois refléter la pratique dans son ensemble. Pour le démontrer, nous évaluerons la pertinence de chacun des critères

[33] Cécile ALVERGNAT (Rapport CNIL présenté par), *Le publipostage électronique et la protection des données personnelles*, 14 oct. 1999, Paris, spéc. p. 1, disponible sur : http://membres.multimania.fr/gretaales/docs/publpost.pdf. – CNIL, *Rapport d'activité 1999*, rapport préc., spéc. p. 108. – Cécile ALVERGNAT (Rapport CNIL présenté par), *Opération « Boîte à spams » : Les enseignements et les actions de la CNIL en matière de communications électroniques non sollicitées*, 24 octobre 2002, rapport préc., spéc. p. 3, disponible sur : http://www.cnil.fr/fileadmin/documents/approfondir/dossier/spam/boite_a_spam.pdf. – Dans une rédaction très proche, Jean FRAYSSINET propose la définition suivante : « *Le spamming ou publipostage électronique sur l'Internet est l'envoi de messages indésirés à des nombres considérables de personnes* […] *à partir de la collecte préalable d'adresses électroniques (e-mail) captées dans les espaces publics de l'Internet (forums de discussions, listes de diffusion, annuaires, sites web) et même parfois de manière illicite grâce à des logiciels " aspirateurs " qui repèrent sur le réseau la circulation d'une adresse e-mail constituant une donnée personnelle* » (« Nouvelles technologies de l'information et de la communication et protection des libertés des consommateurs », *in* Marie-Christine PIATTI, *Les libertés individuelles à l'épreuve des NTIC*, P.U.L., 2001, spéc. pp. 42-43).

[34] Loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, J.O. n° 182 du 7 août 2004, p. 14063 et s.

[35] *Opération « Boîte à spams » : Les enseignements et les actions de la CNIL en matière de communications électroniques non sollicitées*, rapport préc., spéc. p. 4).

[36] TGI Rochefort-sur-Mer, 28 févr. 2001, *Monsieur Christophe G c/ SA France Telecom Interactive*, *Juris-Data* n° 2001-199479 ; *Legalis.net* 2002, n° 3, spéc. p. 114 ; *JCP* 2003, éd. E., chron., 147, spéc. n° 30, obs. J.-M. Bruguière et V. Nisato ; *Comm. com. électr*. avr. 2002, comm. 59, pp. 24-25, obs. L. Grynbaum. – V. ég. TGI Paris, ord. réf., 15 janv. 2002, *Monsieur P. V. c/ Sté Liberty Surf et Sté Free*, *D.* 2002, jurispr., p. 1544 et s., note L. Marino ; *Comm. com. électr*., avr. 2002, 2e esp., comm. 59, p. 24 et s., note L. Grynbaum ; 2003, éd. E., chron., 147, spéc. n° 30, obs. J.-M. Bruguière et V. Nisato ; Juris-*Data* n° 2002-188900 ; *Expertises*, 2002, n° 259, p. 200 (en l'espèce, le *spamming* consistait à « *dépos*[er] *de nombreux messages publicitaires, sur différents forums de discussion en vue de développer ses activités commerciales* »).

proposés par la CNIL au regard de la réalité du *spamming* (a.) et puis tâcherons de rechercher si d'autres critères peuvent caractériser cette pratique (b.).

1. Analyse des critères de définition retenus par la CNIL

13. Des « *envois massifs et parfois répétés* ». De façon pragmatique, la CNIL a intégré dans la définition du *spamming* les caractères « massif » et « répété », par référence aux techniques d'envoi des messages. En effet, le plus souvent, les « spammeurs » ont recours à des logiciels spécialement conçus pour « bombarder » un nombre considérable de messageries électroniques (*spamware*) [37]. Toutefois, si l'on devait retenir ce critère comme élément de définition du *spamming*, cela impliquerait que tout envoi massif serait considéré systématiquement comme du *spamming*. Or, la lettre d'information en est un contre-exemple. Il s'agit en effet de publications diffusées de manière périodique et gratuitement par courrier électronique et adressées à un public déterminé qui s'y est inscrit par le biais d'une formulaire d'abonnement. Par ailleurs, dans la plupart des cas de *spamming*, le caractère massif des envois ne pourra pas être perçu par les « spammés » puisque chaque message sera adressé à un destinataire différent. Ce critère constitue un simple indice de la présence de *spamming* et qui pourra, dans certaines hypothèses, participer à démontrer l'ampleur du dommage. Il en sera ainsi lorsque le « spammé » est la cible de *mail bombing*, c'est-à-dire une attaque qui consiste à envoyer une quantité considérable d'*e-mails* à une même adresse électronique à des fins malveillantes (encombrement de la bande passante entraînant un ralentissement de la connexion à l'internet, engorgement de la messagerie électronique) [38]. L'ensemble de ces observations conduit à conclure que le caractère massif des envois constitue seulement un indicateur permettant de soupçonner l'existence de *spamming*.

14. Le caractère non sollicité des messages. Selon la définition de la CNIL et que l'on retrouve à l'article 22 de la LCEN, le *spam* correspond en pratique à un courrier auquel le destinataire n'a pas consenti à recevoir au préalable. Ce critère permet d'ailleurs de différencier le *spam* d'une lettre d'information, définie comme « *un message envoyé à partir d'un site sur lequel l'internaute s'est préalablement inscrit* » [39], c'est-à-dire que ce dernier a

[37] En doctrine, certains auteurs ont également mis l'accent sur le volume des envois commerciaux (v. par ex. Gérard HAAS et Oivier de TISSOT, « Le publipostage non sollicité dans le collimateur de la justice », *Expertises* 2002, spéc. p. 186).
[38] Sur les atteintes éprouvées par les « spammés », v. *infra* : n° 44 et s.
[39] Disponible sur : http://www.cnil.fr//index.php?id=1269.

donné son consentement à la réception de futurs messages. Ce critère requiert donc un comportement actif du destinataire, à savoir la formalisation de son consentement. Le *spam* serait donc entendu comme un message non sollicité par le destinataire. Ce critère apparaît toutefois insuffisant car si l'on s'arrêtait à ce seul critère de définition, cela reviendrait à considéré tout message non sollicité serait du *spam* puisque beaucoup d'*e-mails* que nous recevons ne sont pas attendus. Afin de préciser ce critère, nous allons examiner l'opération précédent l'envoi de *spams*¸ à savoir la collecte des données nominatives et sur laquelle la CNIL a également pris position.

15. L'indifférence du caractère irrégulier ou déloyal de la collecte. Ici encore, si la CNIL a voulu faire preuve de pragmatisme en visant l'une des hypothèses les plus fréquentes de *spamming.* Toutefois, cette pratique ne peut se limiter à ce seul cas de figure. En effet, il se peut que le « spammeur » ait collecté des adresses électroniques de façon régulière, l'illicéité de la pratique ne se révélant qu'au stade de leur exploitation à des fins d'envois de *spams* [40]. Ce constat conduit donc à écarter ce critère des éléments de définition stables tels que nous les recherchons et à le considérer comme un simple indice faisant présumer la présence de *spamming*. Il convient ainsi de retenir que le *spamming* est caractérisé dès lors que des messages non sollicités sont envoyés à partir de données nominatives utilisées de façon irrégulière, c'est-à-dire sans le consentement préalable de leur titulaire.

16. La captation d'adresses électroniques dans les espaces publics de l'internet. Cet élément de définition visé par la CNIL appelle plusieurs remarques. S'agissant du procédé de collecte, celui-ci correspond à l'une des méthodes principalement utilisées par les « spammeurs »[41]. Ces derniers ont en effet le plus souvent recours à des logiciels de *harvesting* pour collecter massivement des adresses électroniques présentes dans les espaces publics de l'internet (site Internet, forums de discussion, annuaires, listes de diffusion …). Toutefois, d'autres méthodes leur permettent de se procurer des adresses : soit par l'achat de fichiers d'adresses ou la génération automatique [42]. Les termes de « captation » ou de « collecte » apparaissent dès lors incomplets pour décrire les méthodes utilisées par les « spammeurs » pour obtenir ces données. Cette même remarque peut être formulée à propos des adresses électroniques. Si ces dernières constituent à ce jour la matière première du

[40] Rappr. de la question du contact préalable entre l'expéditeur et le destinaire (v. *infra* : n° 17). – À titre de comparaison, il est intéressant de noter qu'aux États-Unis, la simple collecte à l'insu de la personne de son adresse électronique est légale dès lors qu'elle ne porte pas atteinte au principe de loyauté, principe qui gouverne le monde des affaires (*fair practice principle*). Contrairement au système juridique français, seul le caractère déloyal ou trompeur de certaines pratiques fondera les poursuites engagées à l'encontre des « spammeurs ».
[41] V. *infra* : n° 83 et s.
[42] Sur les procédés de collecte des « spammeurs », v. *infra* : n^{os} 92-93.

spamming, par le biais des nouvelles technologies de l'information et de la communication (NTIC), de nouveaux identifiants numériques sont apparus et pourront, à l'avenir, présenter un grand intérêt pour les « spammeurs ». Tel est le cas notamment des données *Bluetooth* qui sont des données permettant à une personne de s'identifier auprès d'une connexion *Bluetooth*, une nouvelle forme de communication sans fil à courte distance [43]. Il convient donc de ne pas limiter les données traitées par le « spammeur » aux seules adresses électroniques mais de viser plus largement toute donnée permettant d'identifier les futurs destinataires.

17. L'indifférence quant au contact préalable. La CNIL définit le *spamming* comme l'envoi de messages à des personnes avec qui « *le destinataire n'a jamais eu de contact* ». Afin d'évaluer la pertinence de ce critère, il convient d'évoquer deux hypothèses distinctes. D'une part, il est des cas où les expéditeurs peuvent n'avoir eu aucun contact avec des internautes mais récupérer leur adresse électronique à partir d'une base de données *marketing* constituée en parfaite conformité avec la loi IFL du 6 janvier 1978 et les utiliser par la suite dans le respect des prescriptions légales. Dans ce cas de figure, la pratique est licite et ne peut caractériser du *spamming*. À l'inverse, l'exploitant d'un site *Web* qui a déjà été en contact avec un internaute et qui a collecté licitement les adresses des visiteurs de son site, peut exploiter ces adresses de manière illicite. Il en sera ainsi, par exemple, lorsque cet exploitant les vend à un tiers sans le consentement préalable des personnes concernées ou les utilise pour des finalités autres que celles initialement prévues. Ces deux hypothèses mettent en évidence que le critère tenant à l'absence de contact préalable entre le « spammeur » et le « spammé » apparaît tout au plus comme indice permettant de soupçonner l'existence d'un cas de *spamming*.

18. L'indifférence quant à la finalité commerciale du message. Contrairement à la LCEN qui limite son champ d'application aux seuls messages à caractère commercial [44], la CNIL retient une définition plus large en soulignant que la finalité commerciale du *spamming* ne constitue que l'une des finalités possibles (« *le plus souvent à caractère commercial* »). Cette position de la Commission doit, selon nous, être saluée. En effet, comme nous le verrons de façon plus détaillée ultérieurement, les dommages causés par le *spamming* sont indépendants de la finalité du message, la gêne éprouvée par les destinataires résultant de la réception incessante de *spams* et non pas de leur finalité. De même, le dysfonctionnement des services de messageries des entreprises ou du réseau des FAI est

[43] Sur ces nouveaux identifiants et les enjeux entourant ces nouvelles données, v. *infra* : n^os^ 187, 192, 197.
[44] V. art. 22 LCEN préc.

indépendant de la finalité du messages, la réception de *spams* pouvant provoquer des conséquences identiques, que le message ait un caractère commercial, politique, caritatif ou encore religieux [45].

19. L'évolution des supports du *spamming*. La CNIL vise le « courrier électronique », défini selon la directive 2002/58/CE, dite « directive vie privée et communications électroniques » [46], comme « *tout message sous forme de texte, de voix, de son, ou d'image envoyé par un réseau public de communications qui peut être stocké dans le réseau ou dans l'équipement terminal du destinataire jusqu'à ce que ce dernier le récupère* ». Cette définition est également reprise par la LCEN, en son article 1er IV : « *On entend par courrier électronique tout message, sous forme de texte, de voix, de son ou d'image, envoyé par un réseau public de communication, stocké sur un serveur du réseau ou dans l'équipement terminal du destinataire, jusqu'à ce que ce dernier le récupère* ». L'adoption d'une acceptation large de la notion de « courrier électronique » est pertinente dans la mesure où nous verrons que le *spamming* ne s'attaque plus uniquement au messagerie électronique par le biais de l'*e-mail* mais cible également, par exemple, les téléphones mobiles sur lesquels seront transmis des *spams* sous la forme de SMS ou MMS ou encore de messages vocaux [47].

20. Premier bilan. À l'issue de cette analyse, la pratique du *spamming* pourrait donc être définie comme l'envoi de courriers électroniques non sollicités, à partir de données d'identification (ou données à caractère personnel [48]), le plus souvent d'adresses électroniques, et dont l'utilisation n'a pas été préalablement autorisée par leurs titulaires, futurs destinataires de ces *spams* [49].

2. La recherche d'autres critères de définition objectifs

[45] Pour des détails sur cette question et les critiques formulées à l'encontre du champ d'application de la LCEN, v. *infra* : nos 300 à 302.

[46] Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques, J.O.U.E. n° L. 201 du 31 juillet 2002, p. 37 et s.

[47] Sur l'évolution des supports du *spamming*, v. *infra* : n° 99 et s..

[48] Sur cette qualification, v. *infra* : n° 58.

[49] Les exemples sur lesquels nous nous appuierons tout au long de nos développements prendront pour référence la collecte d'adresses électroniques, hypothèse la plus fréquente. En revanche, les nouvelles données collectées par le « spammeur » tels que les identifiants *Bluetooth* ne seront que traités dans des parties spécifiques lorsque ce nouveau cas de figure présente certaines particularités qui ont un intérêt particulier pour notre recherche.

21. Au-delà des critères proposés par la CNIL, il convient également de s'interroger sur l'éventuelle pertinence d'autres éléments qui pourraient participer à détecter de façon objective la présence de *spams*.

22. Un critère fondé sur le contenu du message ? La question se pose de savoir quel rôle pourrait jouer le contenu du *spam* dans la recherche d'une définition objective de cette pratique. *Usenet* a été le premier contexte électronique dans lequel certains messages postés au groupe de discussion avaient pu être détectés comme des *spams* en raison de leur contenu. En effet, tout message expédié à un groupe de discussion doit respecter la thématique choisie et tout contenu apparaissant sans rapport avec le sujet traité ou qui s'en éloignerait serait ainsi considéré comme du *spam*. C'est d'ailleurs ce même critère de thématique qui est utilisé pour les *spams* sur les réseaux sociaux et les sites de partage (*Twitter*, *Facebook*, *Youtube*, *Daylimotion*, *MySpace*, …). En revanche, lorsqu'un *e-mail* est envoyé *via* le service de messagerie électronique vers des boîtes aux lettres, il n'existe pas de thème préalablement défini, il peut dès lors traiter de n'importe quel sujet (professionnel, personnel, promotionnel, …). Il convient d'en conclure que ce critère ne doit donc pas être pris en compte dans la définition du *spamming* [50].

23. Un critère fondé sur l'identité de l'émetteur ? La CNIL ne se prononce pas sur la question de savoir si l'anonymat constitue une condition indispensable pour conclure à l'existence du *spamming*. Tous les *spams* ne proviennent pas d'expéditeurs anonymes. Il en est ainsi par exemple, toutes les fois où les messages ont été envoyés à la suite d'un contact préalable avec les destinataires. Toutefois, l'absence d'identification claire de l'expéditeur constitue un indice laissant fortement présumer la présence de *spams*. Comme le souligne la CNIL « *les formes les plus contestées de " spamming " consistent pour l'expéditeur à falsifier ou à masquer son identité ou encore à usurper l'adresse électronique d'un tiers, afin de ne pas être identifié* » [51]. Nous verrons en effet par la suite que le « spammeur » a très souvent recours à divers stratagèmes destinés à éviter d'être tracé [52].

24. Définition retenue. Au regard de l'ensemble des remarques précédentes, le *spamming* devrait être défini comme l'envoi massif de messages non sollicités, par voie

[50] Rappr. des observations faites sur le rejet de la prise en compte de la finalité commerciale du message, v. *infra* n° 300 et s.
[51] CNIL, *Le publipostage électronique et la protection des données personnelles*, rapport préc., spéc. p. 1. – V. ég. Jean FRAYSSINET, « Nouvelles technologies de l'information et de la communication et protection des libertés des consommateurs », *in* Marie-Christine PIATTI, *Les libertés individuelles à l'épreuve des NTIC*, *op. cit.*, spéc. pp. 42-43.
[52] V. *infra* : n° 136 et s.

électronique ou téléphonique, quels que soient leur contenu et leur finalité, en provenance d'un émetteur, connu ou anonyme, et réalisé à partir de données permettant l'identification de leurs titulaires, le plus souvent des adresses électroniques, dont l'utilisation est irrégulière. De façon plus concise, la définition que nous retiendrons au cours de nos travaux est la suivante : **le *spamming* consiste en l'envoi de messages non sollicités à des personnes, à partir de données à caractère personnel utilisées sans le consentement préalable de leur titulaire.** La pratique du *spamming* se décompose ainsi en deux étapes : d'une part, la collecte préalable de données à caractère personnel et d'autre part, l'envoi de *spams* proprement dit.

25. Champ de l'étude. Afin d'appréhender plus facilement cette pratique et les problématiques qu'elle induit, nous partirons de l'hypothèse la plus courante, à savoir : **l'envoi d'*e-mails* non sollicités à partir d'adresses électroniques collectées irrégulièrement dans les espaces publics de l'internet.** L'ensemble des autres indices évoqués précédemment permettront d'envisager les autres hypothèses de *spamming*.

3. La nécessaire prise en compte des diverses formes de *spamming* : l'accroissement des dangers

26. Nous avons adopté une définition volontairement large du *spamming* afin de pouvoir traiter des diverses formes que recouvre cette pratique. En effet, une étude relative au *spamming* ne pourrait être complète si elle ne prenait pas en compte les évolutions qui sont apparues depuis son essor et qui se manifestent à travers des contenus devenus de plus en plus dangereux (a.) mais aussi des méthodes d'envoi de plus en plus agressives (b.).

a. Des contenus plus dangereux

27. Du *spam* commercial au *spam* commercial trompeur. Le *spamming* avait initialement une finalité purement commerciale [53] et était destiné à promouvoir divers produits ou services relatifs à des domaines très variés tels que le secteur financier et de l'épargne (crédits, investissements, assurances, services de réduction de dettes, prêts à taux

[53] Jean-Michel BRUGUIERE observant que la publicité et le *spamming* étant deux pratiques *« intimement liées »* (« La protection du cyber-consommateur dans la loi pour la confiance dans l'économie numérique », *RLDI* janv. 2005, n° 44, p. 59 et s.).

d'intérêt compétitifs etc.), celui de la santé (médicaments, soins, compléments nutritionnels, médecine douce, etc.), de l'informatique (vente de logiciels et de matériel à des prix très compétitifs, hébergement, optimisation de sites *Web*, etc.), celui de l'éducation et de la formation (offres pour des séminaires, stages, cours du soir, etc.), ou encore la pornographie [54]. Les contenus des *spams* se sont par la suite diversifiés en proposant des offres faussement attractives destinées à éveiller la curiosité des destinataires et les inciter à ouvrir ces messages. Des études récentes rapportent qu'une forte majorité de *spams* fait la promotion de produits « miracles » promettant l'amélioration de la virilité, une perte de poids rapide et sans effort, une lutte efficace contre le vieillissement ou encore annonce le gain d'une somme substantielle [55].

28. Le *spamming* propagateur de virus. Parmi les *spams* les plus dangereux, on peut citer ceux qui contenant des virus qui sont intégrés dans le corps du message ou insérés dans une pièce joint [56]. Très fréquemment, ces virus sont destinés à prendre le contrôle à distance du poste infecté et permettre ainsi aux « spammeurs » d'envoyer des *spams* depuis ces ordinateurs (PC zombie) [57].

29. L'association du *spamming* au *phishing*. Le *phishing* ou hameçonnage [58] est une contraction des termes anglais « *fishing* » (pêche) et « *phreaking* » (fraude informatique) [59]. Cette technique de fraude consiste à envoyer un *e-mail* non sollicité à une personne dans le but d'obtenir ses coordonnées confidentielles, le plus souvent ses données bancaires, en se faisant passer pour une société ou une institution financière connues ou un site *Web*, copie conforme du site officiel afin de mettre en confiance le destinataire, et l'inciter à communiquer les informations sollicitées. S'inspirant de ces stratagèmes, le

[54] Selon une étude BITDEFENDER, Les dix principaux contenus du spam au cours du premier semestre 2009 sont les suivants:1. Spam médical ; 2. Liens de phishing ; 3. Emprunts ; 4. Malwares en pièces jointes ; 5. Spam produit / Contrefaçons ; 6. Logiciels/OEM ; 7. Pornographie ; 8. Sites de rencontres ; 9. Emploi ; 10. Diplômes universitaires et Casinos en ligne, disponible sur : http://www.globalsecuritymag.fr/Etude-semestrielle-BitDefender-sur,20090826,12125.html.

[55] V. *infra :* n° 105, 413 et s.

[56] Pour plus de précisions sur cette hypothèse, v. *infra* : n° 104.

[57] V. *infra* : n° 31.

[58] V. Frédéric DUFLOT, « Phishing » : les dessous de la contrefaçon », *RLDI* janv. 2006, n° 366, p. 54 et s. (« *le " phishing " désigne l'obtention des identifiants d'une personne, en se faisant passer pour un individu, une entreprise ou une autorité publique ayant un besoin légitime de solliciter l'information demandée ». Le phishing se caractérise par " la combinaison d'un " social engineering " (une manipulation sociale), et par un ou plusieurs « technical subterfuge " (une manœuvre technologique)* »). – Sur cette technique, v. ég. Éric A. CAPRIOLI, « Le phishing saisi par le droit », *Comm. com. électr*. févr. 2006, comm. 37, p. 47 et s. – David PERE et David FOREST, « L'arsenal répressif du phishing », *D.* 2006, chron., p. 2666. – Pour des détails sur le processus de hameçonnage, v. OCDE, *Document exploratoire sur le vol d'identité en ligne*, DSTI/CP(2007)/3/FINAL, Séoul Corée, 17–18 juin 2008, p. 20 et s., disponible sur : http://www.oecd.org/dataoecd/3/8/40699509.pdf. – Pour des détails sur la connivence entre le *spamming* et le *phishing*, v. *infra* : n° 106.

[59] Éric A. CAPRIOLI, « Le phishing saisi par le droit », art. préc.

« spammeur » envoie de faux *e-mails* afin d'obtenir des données identifiantes ou de les amener à ouvrir les messages contenant des virus [60].

b. Des méthodes d'envoi de plus agressives

30. Le *mail bombing*. La technique du *mail bombing* repose sur l'envoi massif et simultané d'*e-mails* vers une même adresse dans le seul but de nuire au destinataire [61]. Il est essentiel que cette technique soit intégrée dans le cadre de notre étude au regard des lourdes conséquences qu'elle peut avoir pour le « spammé » et qui justifie la recherche d'une protection efficace de la victime dans ce cas de figure précis.

31. Les *Botnets*. Cette méthode d'envoi est la plus redoutable et dangereuse car elle permet aux « spammeurs » de prendre le contrôle d'ordinateurs qui ont été infectés (zombies ou *bots)* par un virus, à l'insu de leur propriétaire. Une fois que le nombre d'ordinateurs compromis (*botnet*) est suffisamment important, le « spammeur », active alors les virus qui commanderont à ces PC zombies l'envoi massif d'*e-mails*, permettant ainsi au « spammeur » d'opérer de façon anonyme [62].

4. Techniques exclues

32. Exclusion de certaines techniques proches mais distinctes du *spamming*. Par le biais des nouvelles technologies, de nombreuses autres techniques sont apparues sur le réseau et qui tendent sur ce point à se rapprocher du *spamming*. Leurs caractéristiques propres en font néanmoins des procédés singuliers qui n'entrent pas dans le champ de notre étude.

33. Le *pop-up* et son dérivé, le *messenger spam*. Les utilisateurs du système *Windows* se voient importunés par l'apparition de fenêtres publicitaires. Par la combinaison du *spam* (message non sollicité) et du *pop-up* (fenêtre qui s'ouvre automatiquement), est apparue une nouvelle méthode de *marketing* électronique qui consiste à adresser un message non sollicité, le plus souvent à caractère publicitaire, par le biais d'un logiciel de messagerie

[60] Sur cette technique d'envoi, v. *infra* : n° 104.
[61] Sur cette attaque, v. *infra* : n° 96.
[62] Sur cette tehnique, v. *infra* : n° 97.

instantanée, tel *Windows Live Messenger* [63]. Ce message, appelé *messenger spam* ou *spam-up*, apparaît sous la forme d'une fenêtre de dialogue qui peut s'ouvrir à tout moment sur l'écran de l'ordinateur lorsque l'internaute est connecté à l'internet [64]. Si le *spam* et le *spam-up* ont en commun d'être des messages non sollicités, ils se distinguent par le procédé d'envoi des messages. En effet, à la différence du *spam* qui est acheminé par courrier électronique, le *pop-up* est quant à lui, expédié par le système d'exploitation *Windows*, les annonceurs exploitant une faille dans le système d'exploitation. La différence avec le *spamming* réside dans la technique de transmission utilisée : alors que le *spam* n'utilise que le logiciel de messagerie électronique, le *messenger spam* peut apparaître quel que soit le logiciel utilisé. Par ailleurs, contrairement aux courriers électroniques qui peuvent être stockés dans un terminal jusqu'à leur consultation par les destinataires, les *spams-up* s'affichent automatiquement lorsque l'internaute est connecté et disparaissent une fois qu'il s'est déconnecté [65].

34. Le *Spamdexing*. Le *spamdexing* ou référencement abusif est la contraction des termes « *spam* » et « *indexing* ». Cette technique consiste à fausser les résultats des moteurs de recherche en ligne. À la différence du *spamming*, aucune donnée à caractère personnel n'est collectée ni aucun message n'est envoyé. Cette technique consiste en effet à recourir à diverses méthodes qui permettent d'améliorer le classement d'un site sur la page de résultats du moteur de recherche en augmentant de façon artificielle le nombre de liens pointant vers le site *Web* considéré. Pour atteindre ce résultat, différentes méthodes sont utilisées comme l'ajout de mots-clés dans les metas tags sans rapport avec la page *Web* consultée, la répétition de mots-clés populaires pour augmenter les chances que le site Internet apparaisse lorsque l'un des mots est recherché (*keywords stuffing*) [66]; le recours à des mots-clés invisibles (même couleur que le fond de la page), …

B. LE *SPAMMING*, AU CARREFOUR D'UNE PLURALITE DE DROITS

[63] Florence SANTROT, « Le " spam-up ", nouvelle plaie du Web », 21 juill. 2003, disponible sur : http://www.journaldunet.com/0307/030721spamup.shtml.
[64] Pour un exemple, v. l'adresse suivante : http://www.stopmessengerspam.com/. V. ég. Florence SANTROT, « Le " spam-up ", nouvelle plaie du Web », art. préc.
[65] La Commission européenne, interrogée sur la qualification de ces fenêtres publicitaires indésirables, a considéré qu'elles n'entraient pas dans la définition du courrier électronique au sens de la directive 2002/58/CE (Question écrite E-3392/02 posée par Astrid THORS (ELDR) à la Commission. Fenêtres publicitaires indésirables dans Windows et protection des données personnelles au sein des réseaux de télécommunication (J.O. n° C 155 E du 3 juillet 2003 pp. 148-149, disponible sur : http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:92002E3392:FR:NOT).
[66] Cette technique est également appelée bourrage de mots-clés.

35. Le droit a vocation à intervenir. À l'origine, le cyberespace a été considéré « *comme un monde rebel à l'emprise du droit* » [67] où primait une liberté d'action absolue, affranchie de toute contrainte légale. Cette conception a été favorisée par les caractéristiques intrinsèques de cet espace que sont l'immatérialité, l'absence de toute frontière physique nationale et surtout le défaut d'autorité supérieure gouvernant l'ensemble. Toutefois, il est désormais admis de façon constante qu'il n'existe pas de vide juridique sur l'internet [68]. Nous verrons à ce titre que la rencontre du droit et du *spamming* s'avère fort riche au regard des nombreux droits que le juriste sera conduit à interroger dans un souci permanent d'assurer une protection efficace des « spammés ».

36. La diversité des droits susceptibles d'être sollicités s'explique en raison de la polymorphie du *spamming* mais également de ses effets, le plus souvent extraterritoriaux. Il conviendra alors d'une part d'interroger le droit positif afin de déterminer quels fondements juridiques pourront intervenir (1.) avant d'aborder le problème dans une perspective internationale (2.).

1. La diversité des droits sollicités

37. La recherche d'une protection efficace à travers la mise en œuvre des lois spéciales. Afin d'identifier quels droits pourront invoquer les « spammés » lorsqu'ils sont victimes de *spamming*, il convient de rappeler à titre préalable que cette pratique se décompose en deux étapes : la première consistant à collecter des adresses électroniques, la seconde correspondant à l'envoi des messages aux titulaires de ces adresses. S'agissant de la collecte d'adresses et de leur utilisation à des fins d'envois, leur réglementation dépendra de la qualification de ces données. À ce titre, la CNIL rappelle expressément que les adresses électroniques sont des données à caractère personnel au sens de la loi IFL [69] : « *une adresse de messagerie électronique est une donnée nominative, soit directement lorsque le nom de l'internaute figure dans le libellé de l'adresse soit indirectement dans la mesure où toute adresse électronique peut être associée à une personne physique* » [70]. Toute opération de

[67] Agathe LEPAGE, « Internet : un nouvel espace de délinquance », *AJ Pénal* juin 2005, p. 217 et s., spéc. p. 217.
[68] Michel VIVANT a clairement affirmé que le droit n'est pas impuissant face aux problématiques qui se posent dans le cybermonde, « *le droit existant pouvant très largement répondre à l'essentiel des difficultés qui peuvent naître, moins du réseau, que de certains comportements qui trouvent à se manifester à travers celui-ci* » (« Cybermonde : Droit et de droits des réseaux », *JCP* 1996, éd. G., I. 396, spéc. n° 10). – Agathe LEPAGE, art. préc., spéc. p. 217 (« *la légitimité du droit à intervenir sur internet non seulement n'est plus contestée, mais s'est même imposée avec la force d'une évidente nécessité* »).
[69] La jurisprudence adopte également cette position, v. *supra* : 186.
[70] CNIL, *Le publipostage électronique et la protection des données personnelles*, rapport préc., spéc. p. 1. – CNIL, *Rapport d'activité 1999*, n° 20, Doc. fr., 2000, spéc. pp. 107-108.

spamming sera dès lors soumise à l'application de cette loi. S'agissant de l'envoi proprement dit, la LCEN est venue encadrer les envois commerciaux et instaure un principe d'interdiction du *spamming* : « [e]*st interdite la prospection directe au moyen d'un automate d'appel, d'un télécopieur ou d'un courrier électronique utilisant, sous quelque forme que ce soit, les coordonnées d'une personne physique qui n'a pas exprimé son consentement préalable à recevoir des prospections directes par ce moyen* » [71]. À travers l'étude de ces deux lois spécifiques, il conviendra, de façon pragmatique, de confronter les solutions que chacune d'elles offrent afin d'évaluer leur efficacité pour protéger d'une part les données à caractère personnel [72], et d'autre part, les « spammés ». Nous verrons que ces lois se révèlent incomplètes pour appréhender la pratique du *spamming* dans son ensemble, en particulier le ses formes les plus dangereuses précédemment recensées [73].

38. La nécessaire recherche d'autres fondements juridiques couvrant les nouvelles formes de *spamming*. Si la LCEN a vocation à réglementer les envois commerciaux, qu'en est-il pour les *spams* qui n'ont pas de vocation publicitaire ? En effet, nous avons vu que le *spamming* ne se réduisait plus à une finalité commerciale était fréquemment associé à d'autres techniques illicites. Certains contenus de *spams* sont ainsi destinés à tromper les destinataires afin de les inciter à ouvrir des messages qui peuvent contenir des virus. D'autres contenus, également trompeurs, vient à obtenir des données identifiantes. D'autres enfin portent atteinte aux systèmes informatiques des victimes. Tel est le cas, par exemple, en cas d'attaque de *mail bombing*. L'ensemble de ces hypothèses renvoient à des comportements illicites qu'il convient de sanctionner. À cette fin, nous interrogerons différents droits pénaux, à savoir : l'escroquerie, le droit pénal de la consommation ou encore le droit pénal de l'informatique. Chacun de ces droits, seront soumis à un examen critique afin d'évaluer leur efficacité face aux différentes hypothèses de *spamming*. Par ailleurs, le *spamming* constitue une pratique dommageable pour les victimes, non seulement au stade de la collecte puisque cette opération est le plus souvent réalisée sans le consentement des titulaires, mais également au stade de l'envoi puisque la réception de *spams* peut être à l'origine de multiples dommages, tels que notamment, l'engorgement du réseau des FAI, le dysfonctionnement des systèmes de messagerie ou encore la saturation des boîtes aux lettres). C'est donc cette fois vers le droit commun de la responsabilité civile que nous nous tournerons afin de déterminer si ce fondement pourrait permettre au « spammé » d'obtenir la réparation du préjudice subi.

[71] Art. 22 LCEN.
[72] Notons que nous utiliserons indifféremment les expressions suivantes : « donnée nominative », « information nominative » et « donnée à caractère personnel » (v. sur ce point, *infra* : n° 184).
[73] V. *supra* : n° 26 et s.

2. Les questions de droit international

39. Une fois que l'on a étudié l'ensemble des droits ayant vocation à s'appliquer selon l'espèce considérée, une autre difficulté de taille devra également être résolue en raison de la dimension internationale du *spamming*.

40. L'internationalité, indissociable du *spamming*. L'internet constitue un formidable outil de communication grâce auquel les personnes, physiques ou morales, quelle que soit leur nationalité ou leur localisation géographique, peuvent entrer en contact et établir des relations. Ces rapprochements produisent naturellement des effets géographiquement localisés sur le territoire de divers États, bousculant ainsi le concept de territorialité, attaché aux notions d'espace et de frontière. L'exemple du *spamming* illustre parfaitement cet éclatement puisque les *spams* sont généralement envoyés à partir d'une source unique vers de multiples destinataires qui peuvent être localisés dans des pays différents.

41. L'intervention nécessaire du droit international privé. Pour régir ces situations à caractère international, le premier réflexe consiste spontanément à créer un instrument contraignant international. Or, le plus souvent, les disparités entre les cultures et systèmes juridiques nationaux [74] empêchent de parvenir à un consensus à l'échelle internationale. À défaut de réglementation juridique internationale, ce sont donc des règles d'origine régionale ou nationale qui ont vocation à s'appliquer. Il apparaît dès lors fort probable que la concurrence de plusieurs lois nationales conduise à des solutions très variées voire antagonistes. Par ailleurs, en l'absence de juridiction supranationale, le contentieux reste porté devant les juridictions nationales avec un risque que plusieurs procédures soient engagées simultanément. De tels conflits en matière de compétences législative et juridictionnelle se posent avec une certaine acuité dans l'hypothèse du *spamming*. En effet, la collecte d'adresses tout comme la réception des *spams* peut survenir dans plusieurs pays. Ainsi, toutes les juridictions et toutes les lois qui auront un lien avec le *spamming* seront susceptibles d'être compétentes pour connaître d'un même litige [75]. Afin d'éviter d'aboutir à de tels résultats impraticables, il convient de déterminer la juridiction compétente et la loi applicable. Le droit international privé se révèle alors incontournable puisqu'il offre une méthode permettant précisément de résoudre de tels conflits.

[74] Sur ces différences, v. *infra* : n° 178 et s.
[75] Peuvent ainsi entrer en concurrence les lois et juridictions des pays d'émission et de réception des *spams*, celles du pays où le « spammeur » et le « spammé » sont localisés et celles de la nationalité du « spammeur » et du « spammé ».

42. Le droit pénal international. Contrairement au droit international privé, il ne s'agit pas d'élire une loi mais de déterminer si une loi donnée est applicable ou non [76]. À l'instar de la plupart des lois pénales, la loi pénale française a vocation à s'appliquer dès lors que l'infraction est commise sur le territoire français. Le principe de territorialité posé par l'article 113-2, alinéa 1er du Code pénal dispose en effet que « [l]*a loi pénale française est applicable aux infractions commises sur le territoire de la République* ». La loi française est également applicable aux infractions réputées commises en France, c'est-à-dire lorsque l'un de leurs faits constitutifs a eu lieu en France [77]. Par exception au principe de territorialité, les articles 113-6 à 113-9 du Code pénal permettent d'appliquer le droit national français lorsque l'infraction est commise hors du territoire français, si l'auteur du délit est de nationalité française (compétence personnelle active) ou si la victime est de nationalité française (compétence personnelle passive). En matière de compétence active, la loi française et la juridiction française sont compétentes pour des délits commis hors de France si les faits sont également punis par la législation du pays où ils sont commis (principe de double incrimination) [78]. En matière de compétence personnelle passive, la victime française d'un délit commis à l'étranger pourra se prévaloir des dispositions de droit français pour poursuivre le délinquant, sous réserve que l'infraction qui a justifié le déclenchement de l'action pénale constitue un délit puni d'une peine d'emprisonnement. Le champ d'application extrêmement large de la loi pénale française lui permet donc d'être reconnue compétente dès lors que le « spammeur » ou les « spammés » sont de nationalité française. En définitive, il en résulte qu'une infraction dont les effets s'étendent sur le territoire de plusieurs États est susceptible de faire intervenir l'application de plusieurs lois nationales, sous réserve du principe *non bis in idem*. Il est dès lors à craindre que le principe de la souveraineté nationale conduise chaque État à ne pas tenir compte du pouvoir répressif des autres États et donc que le jugement rendu par une juridiction nationale soit purement et simplement ignoré par les autres États. Ce constat conduit à la nécessaire désignation d'une juridiction compétente et d'une loi applicable. Intimement liés par cette double problématique, le droit pénal et le droit civil tendent ainsi à se rapprocher. Afin de résoudre les questions de compétence juridictionnelle et législative, nous nous attacherons donc aux seules solutions offertes par le droit international privé [79].

[76] Michel VIVANT, « Cybermonde : droit et droits des réseaux », art. préc. (« *puisque la démarche à suivre n'est plus naturellement bilatérale mais (quasi) nécessairement unilatéraliste* »).
[77] Art. 113-2, al. 2 C. pén.
[78] Art. 113-6 C. pén.
[79] V. André HUET, Le droit pénal international et Internet, *LPA* 10 nov. 1999, n° 224, p. 39 et s.

§ 2. LES INTERETS DE LA RECHERCHE

43. L'intérêt de cette recherche est double. D'un point de vue pratique, nous verrons que le *spamming* est générateur de dommages et justifie un besoin de protection des « spammés » (A.). D'un point de vue théorique, la confrontation du *spamming* et du droit se révèlera être une source de réflexions particulièrement riche. S'inscrivant dans une problématique plus générale qui consiste à déterminer comment le droit est amené à appréhender et à traiter un tel phénomène technique, cette question sollicitera l'imagination et la sagacité du juriste et le contraindra à rechercher des réponses adaptées face aux problèmes spécifiques qui se posent (B.) [80].

A. L'INTERET PRATIQUE : UN BESOIN DE PROTECTION DES « SPAMMES »

44. Le *spamming* est une pratique, par nature, diffuse. Le « spammeur » a le plus souvent recours à des logiciels de *push* permettant d'envoyer massivement des *e-mails* non sollicités à de multiples destinataires. Grâce à ce procédé, le « spammeur » peut ainsi répandre une multitude de messages qui constitue autant de points de contact différents issus d'une source unique. Si la réception de *spams* est susceptible de causer différents dommages aux « spammés », leur identification précise nécessite tout d'abord de déterminer la dimension du *spamming* prise en référence. Deux cas de figure sont possibles : soit on raisonne à partir de son impact général, c'est-à-dire en prenant en compte son effet diffus, soit on raisonne à partir de son impact individuel et donc centré sur la relation « spammeur »/« spammé » pour ne s'intéresser qu'à l'effet produit sur cette seule victime. Afin de rechercher une protection efficace des « spammés » selon le cas de *spamming* considéré, notre étude s'attachera à cette seconde branche de l'alternative. Deux raisons justifient ce choix. D'une part, il nous permettra d'envisager les cas de *spamming* les plus fréquents où, lors d'une même opération d'envois massifs, chaque destinataire ne recevra en réalité qu'un seul *spam* provenant du même « spammeur ». D'autre part, il nous permettra d'examiner des hypothèses particulières comme celle où le « spammeur » a pour dessein de porter atteinte à une seule et même personne en inondant sa messagerie électronique de *spams*. Toutefois, afin d'offrir une vision d'ensemble sur les différentes conséquences du *spamming* et de saisir l'ampleur des dommages que peut causer cette pratique, nous

[80] Si la distinction pratique/théorique peut être discutée, nous avons toutefois fait le choix de la retenir pour des raisons didactiques (sur cette discussion, v. notamment Michel VIVANT, « Sciences et praxis », *D.* 1993, chron., p. 109 et s.

analyserons tout d'abord son impact général (1.) avant d'envisager son impact individuel (2.).

1. L'impact général

45. Nous verrons que le *spamming* porte atteinte aux FAI et aux fournisseurs de messagerie électronique [81] mais également aux entreprises publiques comme privées [82] en raison des coûts financiers significatifs qu'il engendre. Le traitement du *spamming* implique en effet des dépenses tant humaines, techniques que financières qui sont reportées sur les FAI et les destinataires [83]. En 2009, le coût du *spamming* était évalué à 130 milliards de dollars à travers le monde, dont 42 milliards de dollars sur le seul territoire des États-Unis [84]. Si les conséquences financières sont mineures pour les internautes, la réception importante et quotidienne de *spams* est également synonyme de dommage. Ainsi, convient-il de décrire de façon plus détaillée les impacts qu'engendre le *spamming* non seulement sur les entreprises et les FAI (a.) mais également sur les internautes (b.).

a. L'impact sur les entreprises et les FAI

46. Les coûts du *spamming*. Plusieurs études ont été réalisées sur les coûts du *spamming* mais nous porterons une attention plus particulière à celle publiée en 2009 par le

[81] Ces deux organismes sont le plus souvent une seule et même entreprise : les FAI proposent en effet le plus souvent également un service de messagerie électronique. Dans un souci d'alléger nos développements, nous désignerons donc ces deux organismes sous le terme « FAI ».

[82] V. not. Ben DAHL, " A Further Darkside to Unsolicited Commercial Email? An Assessment of Potential Employer Liability for *Spam* Email ", 22 *J. Marshall J. of Comp. & Info. L.* 179 (2003) (soulignant que la prolifération de *spams* sur les lieux de travail constitue une menace importante pour le monde des affaires).

[83] V. *supra* : n° 8.

[84] Ce qui représente une hausse globale des coûts de 30% par rapport à 2007 (consultez l'adresse suivante : http://www.ferris.com/research-library/industry-statistics/). – La société VADE RETRO TECHNOLOGY, expert en protection de systèmes de messagerie électronique, propose de calculer le coût du *spamming* en termes de perte de productivité d'une part et de coûts informatiques d'autre part, ce calcul permettant ainsi d'évaluer, de façon plus concrète, ce que représente le *spamming* en charges financières pour les entreprises victimes de cette pratique. Pour entreprendre cette simulation, nous avons pris comme référence une entreprise de 200 salariés, au salaire annuel moyen de 40.000 euros et recevant chacun en moyenne vingt-cinq *e-mails* par jour, dont 70% du nombre d'*e-mails* reçus sont des *spams*. L'opérateur calcule tout d'abord la perte de productivité de l'entreprise à partir de ces trois paramètres : sur une base de calcul de 5 secondes par *spam*, chaque employé perd annuellement 5,59 heures à trier les messages reçus ; auxquelles s'ajoute l'effet de tentation estimé en moyenne annuellement à 1,34 heures, sur une base de calcul fixée à 20 minutes de perte de temps par *spam* sur 1000 ; soit une perte de temps annuelle estimée à 6,93 heures par employé, ce qui représente une charge annuelle pour l'entreprise évaluée à 30.138,89 euros. En terme de coûts informatiques, le transfert et le stockage des *spams* implique une charge de 40,25 euros par employé, sur une base de calcul fixée à un centime d'euro par *spam*, ce qui implique un coût informatique supplémentaire annuel pour l'entreprise chiffré à 8.050 euros. Au final, le *spamming* coûte annuellement à cette entreprise 38.188,89 euros (« Calculateur du coût du *spam* », disponible sur : http://www.antispam.fr/fr/spam_calculator.asp).

site Internet <altospam> [85] et dans laquelle sont détaillées les différentes composantes de ce coût qui peuvent, dans certains cas, être communes aux entreprises et aux FAI[86].

47. La diminution de la productivité des salariés [87]. La réception massive de *spams* contraint les salariés d'une entreprise à consacrer quotidiennement du temps pour relever l'existence de *spams*, les supprimer de leur boite de réception, vérifier les messages placés en quarantaine, se désabonner ou encore tenter de trouver l'adresse du destinataire. L'attention des salariés, mobilisée au traitement du *spamming* provoquera une perte de temps certaine et, selon le volume de *spams* reçus, pourra avoir des répercussions négatives sur leur productivité.

48. La hausse des coûts du personnel. Le *spamming* pourra également engendrer des coûts du personnel, notamment lorsque l'entreprise décidera de recruter une personne qui aura pour mission de gérer et résoudre les conséquences néfastes du *spamming*. Elle sera, à ce titre, chargée de gérer les problèmes techniques, de mettre en place et d'entretenir l'infrastructure anti-*spam* (paramétrage, formation, maintenance, etc.), d'assister les salariés qui rencontreraient des difficultés, notamment en cas de perte d'*e-mails* légitimes, et de répondre aux plaintes des clients.

49. Les coûts d'infrastructure et de sécurité. La réception massive d'*e-mails* dégrade l'efficacité du réseau informatique et des services de messagerie électronique. Afin de tenter de neutraliser de tels effets, les entreprises sont contraintes d'acquérir des outils anti-*spam* ou des mises à jour supplémentaires. Le *spamming* a également un impact direct sur les FAI puisqu'ils doivent engager des dépenses supplémentaires pour s'assurer que les capacités d'utilisation de leur réseau ne seront pas affectées. À cette fin, ils doivent notamment financer les frais engendrés par la mise en place de dispositifs techniques de protection et l'installation d'une assistance technique. À ces coûts, s'ajoutent ceux relatifs aux mises à jour et à l'amélioration de l'infrastructure existante afin de faire face aux menaces qui s'intensifient. En particulier, l'accroissement exponentiel du trafic et des

[85] ALTOSPAM est un service de la société OKTEY, spécialisée dans l'édition de logiciel anti-virus et anti-*spam* (v. le site disponible sur : http://www.altospam.com/fr/societe.php).
[86] ALTOSPAM, « Les conséquences du *spamming* », actualité 2009, disponible sur : http://www.altospam.com/actualite/2009/06/les-couts-economiques-du-spamming/ – V. IUT, *Financial Aspects of Network Security: Malware and Spam*, Final Report 2008, disponible sur: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-study-financial-aspects-of-malware-and-spam.pdf).
[87] V. ég. FERRIS RESEARCH, *The Global Economic Impact of Spam*, 2005, Report 409, févr. 2005, disponible sur : www.ferris.com.

données à stocker les contraint à engager des frais pour élargir la bande passante et augmenter la capacité d'espace de stockage des messages sur le réseau [88].

50. Perte des revenus escomptés. L'afflux massif de *spams* peut perturber le fonctionnement du système de traitement des *e-mails*. L'engorgement, voire la saturation des boîtes aux lettres électroniques risquent de compromettre la conclusion de contrats commerciaux et d'entraîner la perte de certains *e-mails* légitimes classés à tort comme des *spams* par le logiciel de filtrage (faux positifs) [89]. Cette situation peut engendrer des conséquences financières graves puisque le chiffre d'affaires des entreprises victimes est susceptible de subir une baisse significative.

51. L'atteinte à l'image et à la réputation. La perturbation du système de courrier électronique d'une entreprise (ralentissement, voire paralysie totale) nuit gravement à l'image de cette dernière qui devient notamment incapable d'honorer efficacement ses objectifs commerciaux. Les conséquences supportées par une entreprise peuvent donc être relativement lourdes et s'aggraver lorsque les clients, exaspérés par la gêne occasionnée, vont parfois jusqu'à rompre le contrat, entraînant alors une baisse des recettes. Ce constat se vérifie d'autant plus à l'égard des FAI dont l'image repose sur la disponibilité de leur réseau et l'efficacité de leur service de messagerie.

b. L'impact sur la communauté des internautes

52. L'irritation, la gêne. En raison de la quantité importante de *spams* reçus quotidiennement dans leurs boîtes aux lettres électroniques, les particuliers subissent également les effets du *spamming*. Le temps consacré à trier et à supprimer les *spams* et la répétition systématique de cette tâche suscite la gêne voire l'exaspération des internautes [90]. La réception d'un grand nombre de *spams* peut également ralentir significativement la vitesse de connexion ou encore engendrer un encombrement des boîtes aux lettres électroniques, la capacité de stockage des *e-mails* étant limitée. Lorsque le volume de *spams* reçus est trop important, le système informatique des destinataires peut alors être bloqué, la

[88] David SORKIN, *Technical and Legal Approaches to Unsolicited Electronic Mail*, art. préc.
[89] V. *infra* : n° 172 et s.
[90] Précisons que tous les internautes qui reçoivent des *spams* sont victimes d'une atteinte à leurs données à caractère personnel dès lors que la collecte a été opérée selon des procédé illicite. Toutefois, par souci de clarté de nos propos, nous avons fait le choix de mettre l'accent, dans la dimension collective du *spamming*, sur les conséquences engendrées par l'envoi massif de *spams* afin de réserver l'atteinte aux données dans le cadre du *spamming* individuel puisque notre recherche se concentrera sur cette seule hypothèse.

mémoire vive requise pour ouvrir certains *spams* étant si importante qu'il n'est plus possible de donner des ordres d'exécution différents. Ces effets ont donc inéluctablement une incidence directe sur la perte d'efficacité et de fiabilité du système de messagerie électronique. Enfin, la réception massive de *spams* est susceptible d'entraîner une perte d'attention des internautes, les messages légitimes, noyés dans un flot de *spams*, risquent d'être perdus, effacés ou ignorés.

53. La perte de confiance envers le commerce électronique. L*e spamming* a également un impact sur le commerce électronique en érodant la confiance des consommateurs et les transactions sécurisées. En effet, une forte proportion d*e spams* est liée à des activités commerciales à caractère frauduleux, trompeur ou pornographique qui accroît la méfiance des internautes envers les services de courriers électroniques. De façon plus générale, cette méfiance se répercute également à l'égard de l'internet et du commerce électronique alors même que la confiance des acteurs de l'internet est une condition *sine qua non* au développement du commerce électronique et de la société de l'information. Enfin, l'inquiétude des internautes se manifeste également dans leur choix lors d'opérations réalisées en ligne. À cette occasion, ils préfèrent accorder leur confiance à de grandes entreprises déjà connues au détriment de petites sociétés émergentes qui subissent inévitablement un ralentissement de leur activité.

2. L'impact individuel

54. Contrairement à l'hypothèse précédente, il s'agit ici de restreindre le champ de notre étude au différend opposant un « spammé » à un « spammeur ». Dans ce contexte précis, le changement d'échelle spatiale conduit à identifier précisément le ou les dommages subis par une victime de *spamming* et qui détermineraient cette dernière à engager des poursuites contre le « spammeur ». Suivant la démarche précédemment adoptée, nous définirons, les effets du *spamming* sur un « spammé », selon que ce dernier est une entreprise, un FAI (a.) ou un internaute (b.) en raisonnant à partir de différents cas de figure. Sans traiter l'ensemble des cas de *spamming* de manière exhaustive, les hypothèses retenues nous permettrons d'offrir une vision relativement complète des principales difficultés auxquelles un juriste peut être confronté lorsqu'un « spammé » sollicite ses conseils. À l'aune de ces exemples, nous pourrons ainsi évaluer par la suite la pertinence et l'efficacité de chacun des fondements juridiques possibles.

a. L'impact sur un « spammé », entreprise ou FAI

55. Si le « spammeur » envoie le plus souvent des *spams* de façon aléatoire à de multiples destinataires, il est des cas où, après avoir récupéré les adresses électroniques d'une importante quantité de salariés de cette entreprise, il procèdera à l'envoi de *spams* à destination de cette entreprise unique. Ces envois multiples sont susceptibles de perturber le fonctionnement du système de messagerie. Mais les conséquences peuvent être encore plus graves lorsque le « spammeur » entreprend une opération de *mail bombing* [91] puisque ce type d'opérations peut entraîner l'interruption des services de messagerie. Leur dysfonctionnement risque d'engendrer la perte d'*e-mails* importants qui auraient pu sans doute lui permettre de conclure un futur contrat ou de poursuivre une négociation engagée avec un nouveau client. Quelque soit le cas de figure, la réception trop importante de *spams* peut perturber la productivité des salariés et contraindre l'entreprise à engager des coûts supplémentaires pour maintenir la capacité de traitement de son système informatique. On retrouve alors les conséquences du *spamming* évoquées lors de l'étude de son impact général [92].

56. De façon indirecte, les FAI peuvent également souffrir du *spamming*. Il en est ainsi chaque fois que le « spammeur » utilise le réseau du FAI pour « bombarder » de *spams* ses abonnés. Ces envois massifs peuvent alors fortement perturber son réseau et encombrer sa bande passante. Mais les effets peuvent encore être plus dommageables lorsqu'il devient la cible directe du « spammeur ». Tel est le cas lorsqu'il est victime d'une attaque de *mail bombing* puisqu'elle peut entraîner la paralysie de son réseau et la saturation sa bande passante. Dans ce cas de figure, le FAI se voit contraint de stocker temporairement un important volume d'*e-mails* qui occupe alors l'espace de stockage du système. Les capacités de traitement des messages se trouvent ainsi fortement diminuées puisqu'une importante partie de son système informatique est mobilisée pour retourner les *e-mails* ou stopper les futurs messages provenant de ce « spammeur », l'empêchant ainsi de satisfaire les demandes de ses abonnés en termes d'acheminement des *e-mails* et de connexion à l'internet. Cette situation peut engendrer des préjudices économiques plus ou moins graves sur son chiffre d'affaires. En effet, de tels dysfonctionnements techniques peuvent porter atteinte à sa réputation commerciale et conduire certains abonnés mécontents à résilier le contrat et l'exposera ainsi à un manque à gagner certain.

[91] V. *supra* : n° 30.
[92] V. *supra* : n° 46 et s.

b. L'impact sur un « spammé », internaute

57. Le « spammé » particulier subira deux types d'atteintes pouvant justifier la poursuite du « spammeur » : l'une résultant d'une atteinte à ses données à caractère personnel (i.), l'autre découlant de l'envoi de *spams* proprement dit (ii.).

i. La menace sur les données à caractère personnel

58. Les données à caractère personnel, des données d'identification indispensables au *spamming*. À l'instar de toute correspondance, le « spammeur » doit disposer d'informations permettant l'identification des futurs destinataires de ses messages afin de s'assurer qu'ils parviennent à ces derniers. La fonction d'identification jouée par ce type de données est donc essentielle puisqu'elle conditionne l'intérêt que le « spammeur » leur portera. La fonction d'identification apparaît dès lors comme une notion centrale dont il convient de saisir la portée. De façon positive, la notion d'identification recouvre deux aspects : elle est à la fois un instrument y concourant et le résultat de ce processus, à savoir dévoiler « *l'identité individuelle qui nous permet de nous distinguer de notre voisin* » [93], et composée d'un « *ensemble de composants grâce auxquels il est établi qu'une personne est bien celle qui se dit ou que l'on présume telle* » [94]. Les données à caractère personnel remplissent précisément ce rôle d'identification puisqu'il s'agit, selon la loi française, de « *toute information relative à une personne physique identifiée ou qui peut être identifiée* » [95]. Cette définition consacre donc une acception large des données considérées comme identifiantes [96] : dès l'instant où il existe un lien suffisamment étroit entre une donnée et une personne permettant à la première l'identification directe ou indirecte de la seconde [97]. Il s'ensuit que toute information même indirectement nominative a vocation à

[93] Fanny VASSEUR-LAMBRY, *L'identité de la personne humaine*, *LPA* 6 mai 2004, n° 91, p. 5 et s. (l'identité est composée de deux versants, un versant « *individualiste* » qui « *recouvre l'identité individuelle qui nous permet de nous distinguer de notre voisin* » et un versant « *communautaire* » qui « *permet de nous identifier à la communauté à laquelle nous appartenons et qui assure la cohésion du groupe* »).

[94] Serge GUINCHARD et Thierry DEBARD, *Lexique des termes juridiques*, 18e éd., Dalloz, 2011, v. « identification ».

[95] Art. 2 al. 2 de la loi du 6 août 2004. – Dans une rédaction similaire, les textes législatifs qui la précédent adoptent également une interprétation large de cette notion. Selon l'article 4 de la loi IFL du 6 janvier 1978, « *sont réputées nominatives au sens de la présente loi les informations qui permettent, sous quelque forme que se soit, directement ou non, l'identification des personnes physiques auxquelles elles s'appliquent* ».

[96] Sur cette acceptation large de la notion de données à caractère personnel, v. *infra* ° 185.

[97] Sont notamment des données à caractère personnel le nom, le numéro de compte bancaire, les données anthropomorphiques, la photographie, la voix, l'image. – À propos de l'image, v. TGI Privas, 3 sept. 1997, *Rev. sc. crim.* 1998, p. 574, obs. Francillon ; *LPA* 11 nov. 1998, n° 135, p. 19 et s., obs. J. Frayssinet (reconnaissant pour la première fois l'image comme une donnée à caractère personnel et confirmé par l'arrêt de la CA Nîmes, 6

être protégée et ce, quel que soit le niveau de précision et de certitude quant à son rattachement avec la personne concernée [98]. Cette acception large de la notion de données à caractère personnel permet ainsi d'englober des identifiants issus des NTIC [99], et notamment l'adresse électronique [100]. Pour répondre à cet impératif d'identification [101], l'adresse électronique joue un rôle fondamental au sein de l'échange d'informations entre les internautes, au même titre que celui assuré par l'adresse postale physique. La fonction d'identification assurée par l'adresse électronique la rend dès lors indispensable à l'envoi des messages et justifie ainsi tout l'intérêt que manifestent les « spammeurs » à son égard.

59. La capture des adresses électroniques dans les espaces publics de l'internet : le véritable enjeu en termes de protection. Le « spammeur » peut se procurer des adresses auprès de tiers à qui il achètera des bases de données, il peut encore les créer automatiquement [102] mais le plus souvent, il procédera à leur collecte grâce à divers procédés. Parmi eux, certains sont susceptibles d'engendrer une menace pour ces données. Selon la CNIL [103], la collecte de ces données peut être réalisée à partir de trois types de ressources [104]. La première méthode consiste à les récolter directement grâce à des fichiers constitués à partir de données nominatives communiquées volontairement par les internautes avec lesquels le prospecteur s'est trouvé en contact direct. L'internaute est en effet appelé à révéler son adresse électronique à l'occasion de très nombreuses opérations effectuées en

nov. 1998, *M. F. c/ Le Ministère Public et Melle S.*) – V. ég. Jean FRAYSSINET, note sous TGI Privas, 3 sept. 1997, jugement préc. (soulignant que « [c]*e qui importe* […] *c'est le point de savoir si les données permettent ou non, avec un degré suffisant, l'identification de la personne concernée. Les données peuvent avoir la forme d'une image, d'un texte* […] *ou d'un son (la voix)* »).

[98] V. par ex. à propos de l'image, TGI Paris, 13 mars 1991, *Juris-Data* n° 1991-045872 (jugeant qu'un instrument audiovisuel captant l'image de personnes sur un lieu de travail, à leur insu, est considéré comme portant atteinte à leur droit à l'image alors même que le visage de ces salariés avaient été, à l'occasion de la publication, dissimulé sous un cache dans la mesure où « *ils étaient facilement identifiables à raison des prises de vue très précises de la boutique et de son enseigne* »).

[99] Les identifiants numériques *« peuvent se définir comme autant de signes qui caractérisent un individu de son point de vue, partiellement ou totalement, de manière définitive ou temporaire, dans un contexte électronique* » (Olivier ITEANU, *L'identité numérique en question*, Eyrolles, 2008, spéc. p. 5).

[100] Comme nous l'avons indiqué précédemment, la CNIL, tout comme les juges, considèrent clairement l'adresse électronique comme une donnée à caractère personnel (sur ce point, v. *supra* : n° 37 et 186).

[101] L'importance attachée à cette fonction d'identification est clairement exprimée par Fanny VASSEUR-LAMBRY : « *Cette obligation d'identification s'impose non seulement dans l'intérêt de la société, mais elle est aussi nécessaire pour chaque individu. En effet, à défaut d'identification, un être humain est juridiquement inexistant, donc dépourvu de toute personnalité juridique. Autrement dit, toute vie sociale lui est interdite, il ne peut accomplir aucun acte juridique, il est tout simplement privé de ses libertés* » (*L'identité de la personne humaine*, art. préc.

[102] Sur cette technique, v. infra : n° 93 – Cette technique ne retiendra toutefois pas notre attention dans la mesure où rien n'assure que ce type de données correspondera à à une personne identifiée ou identifiable. Dans ce cas de figure, l'expédition de messages à ces adresses ne risquera d'entraîner aucune gêne ni aucun dommage. Pour des raisons didactiques, nous nous concentrerons donc sur le cas le plus fréquent et qui permet d'illustrer concrètement les menaces pesant sur les données à caractère personnel, à savoir l'hypothèse de la collecte.

[103] http://www.cnil.fr.

[104] CNIL, « La véritable portée du problème : la collecte des *e-mails* dans les espaces publics de l'Internet », *in* CNIL, *Le publipostage électronique et la protection des données personnelles*, 14 oct. 1999, rapport préc., spéc. pp. 19-20.

ligne : lors d'une inscription sur un site *Web*, de la formulation d'une requête, d'un abonnement à une liste de diffusion, d'une commande passée sur un site marchand, lorsqu'il remplit un formulaire en ligne, etc. [105]. Dans tous ces cas de figure, la collecte directe des données auprès des personnes concernées ne porte pas atteinte à la protection de leurs données à caractère personnel dès lors qu'elles ont été informées de la collecte initiale de leurs données et mises en mesure d'exercer leur droit d'opposition au traitement de leurs données à des fins de prospection commerciale ou à leur cession à des tiers. À l'inverse, cette collecte peut être opérée de façon indirecte, à partir de listes d'adresses électroniques fournies par un tiers par le biais d'une cession, par exemple. Les garanties de licéité de la collecte sont assurées si, comme dans le premier cas, les personnes concernées ont été informées que leurs données pourront être communiquées à des tiers à des fins de prospection et qu'elles ont été en mesure de s'opposer à cette éventuelle cession. Mais, bien souvent, cette opération s'effectue de façon « sauvage » dans les espaces publics, au moyen de « logiciels aspirateurs » permettant de collecter massivement les adresses électroniques divulguées par l'internaute. En effet, à l'occasion de ses connexions successives au réseau, l'internaute laisse de multiples traces, et notamment son adresse électronique [106]. Des sites consultés aux commentaires laissés sur un forum de discussion ou sur les annuaires diffusés sur des sites *Web*, en passant par la publication de *blogs*, l'inscription à des listes de diffusion ou encore la participation à des sites participatifs (plateformes de partage ou site communautaire) ; toutes ces opérations requièrent la communication d'une adresses électronique. L'ensemble de ces espaces publics de l'internet devient ainsi la cible privilégiée des « spammeurs » [107]. Ce sont de telles méthodes de collecte « sauvage » qui ont été dénoncées par la CNIL comme portant atteinte aux données à caractère personnel [108] et contre lesquelles il convient de protéger les données.

ii. L'atteinte subie par la réception d'un spam

60. Afin de déterminer les dommages que peut invoquer un « spammé » et susceptibles de déclencher des poursuites à l'encontre du « spammeur », il convient de garder à l'esprit que nous raisonnons sur le cas précis où le ou les messages reçus par un « spammé » proviennent d'un seul et même « spammeur ». Dans ce cas de figure, il pourra difficilement se plaindre d'un réel préjudice découlant notamment de la gêne occasionnée

[105] V. *infra :* n° 83.
[106] Sur les multiples traces laissées par les internautes, v. *infra* : n° 165.
[107] Sur ce point, v. *infra :* n° 83.
[108] CNIL, *Le publipostage électronique et la protection des données à caractère personne*, rapport préc., *loc ; cit.*

par cette réception. En effet, ce sentiment de dérangement, voire d'exaspération, résulte non pas de la réception de ce message unique mais de la réception multiple et incessante d'*e-mails* non sollicités. Faute de pouvoir obtenir la réparation d'un prétendu préjudice, « le spammé » pourra rechercher la sanction du « spammeur » en raison du contenu du *spam* reçu. En effet, comme nous l'avons vu précédemment, les *spams* peuvent contenir des informations publicitaires de nature à tromper leurs destinataires afin de les inciter à ouvrir un message contenant, parfois, un virus ou de les conduire à révéler certaines de leurs informations nominatives [109]. La victime pourrait alors envisager d'engager des poursuites pénales contre le « spammeur » soit sur le fondement de la publicité trompeuse [110], soit sur celui de l'escroquerie [111] selon l'espèce considérée. Dans deux hypothèses toutefois, l'importance des dommages subis par le « spammé » pourra justifier une demande en réparation. Il en pourra en être ainsi d'une part lorsque ce dernier est victime d'une attaque de *mail bombing* provoquant la saturation de sa messagerie électronique [112]. À l'instar des entreprises ou des FAI victimes de ce même type d'attaque, il pourrait en effet subir, à la suite de cette saturation, la perte d'une chance de consulter des *e-mails* importants qui n'auraient jamais pu être acheminés [113]. Parallèlement à cette action en indemnisation, il pourra également envisager une action pénale pour l'atteinte portée à son système informatique [114]. D'autre part, le « spammé » pourra également subir un dommage important appelant réparation dans le cas où l'internaute est victime de piratage informatique (PC zombie). Devenant, à son insu, l'expéditeur officiel des *spams*, chacun des destinataires mécontents risque de lui retourner l'*e-mail* reçu, provoquant ainsi la saturation de sa messagerie électronique et le blocage des *e-mails* entrants [115]. Outre cette action en réparation, le « spammé » pourra également envisager des poursuites pénales pour l'atteinte portée à son système informatique [116]. Il en résulte que, hormis les hypothèses de *mail bombing* et de PC zombie qui peuvent constituer à la fois un délit pénal et civil, dans le cas le plus fréquent où le « spammeur » envoie le même message à un nombre important de destinataires, l'action destinée à obtenir l'indemnisation du prétendu dommage subi semble compromise ; la seule issue restant alors de rechercher si des poursuites pénales sont envisageables.

[109] V. *supra* : n° 27 à 29.
[110] Art. 121-1 et s. C. conso. – V. *infra* : n° 413 et s.
[111] Art. 313-1 C. pén. – V. *infra* : n° 384 et s.
[112] V. *infra* : n° 452.
[113] V. *infra* : n° 455.
[114] Art. 323-1 et 313-2 C. pén. – V. *infra* : n^{os} 375 et 381.
[115] V. *infra* : n^{os} 452 et 455.
[116] Art. 323- 1 C. pén. – V. *infra* : n° 375.

B. L'INTERET THEORIQUE : LE DROIT FACE AUX NOUVELLES TECHNOLOGIES

61. La rencontre de deux mondes. Les progrès scientifiques ont influencé de tout temps le droit, chaque évolution technique ayant eu des répercussions plus ou moins importantes sur le droit [117]. Le droit n'a en effet pas été insensible à l'invention de l'imprimerie, à la révolution industrielle, aux innovations en matière de transport, ou encore aux diverses évolutions en matière de transmission des informations (télévision, radio, fax, téléphone…). L'esprit du droit a été ainsi « *transposé dans une tonalité nouvelle, plus matérialiste, plus pragmatique* » [118]. Cette évolution s'est notamment manifestée travers un phénomène de « complexification » [119] du droit qui s'est traduit par une multiplication des lois spéciales destinées à répondre à des problèmes spécifiques. L'utilisation croissante de l'automobile, par exemple, a été à l'origine de multiples dommages qui ont nécessité une intervention du droit [120]. Plus tard, l'informatique a également engendré des difficultés juridiques qui ont appelé une intervention du droit. Ces exemples démontrent sans conteste que le droit entretient des rapports étroits avec les réalités socio-économiques [121].

62. Quelle est l'influence du fait sur le droit ? En raison de ce lien qui unit le droit et un fait (économique ou social) qui lui est extérieur, la question se pose de savoir si le droit doit entériner un fait de façon mécanique ou bien l'orienter. Admettre la première alternative de cette option reviendrait à amputer le travail du législateur de l'une de ses missions. En effet, lors de l'élaboration d'une loi, le législateur ne peut se cantonner à accepter des faits parce qu'ils existent : on lui demande de faire des choix, de s'imposer [122]. Ainsi, la finalité du droit ne saurait se limiter à mettre en forme les faits en collant

[117] V. en ce sens notamment Pierre CATALA, « Unité ou complexité », *in Droit et informatique : L'hermine et la puce,* (préf. Jean CARBONNIER), Masson, coll. *Frederick R. Bull*, 1992, spéc. p. 4. – Jérôme HUET, « Droit, informatique et rationalité », *in Droit et informatique : L'hermine et la puce, op. cit.,* spéc. p. 82.

[118] Louis JOSSERAND, « Un ordre juridique nouveau », *D.H.* 1937, chron., p. 41.

[119] Pour différentes réflexions sur cette complexification du droit, v. not. Jacques BEGUIN, « Peut-on remédier à la complexité croissante du droit ? », *in Mélanges en l'honneur de Henry Blaise*, Economica, 1995, p. 1 et s. – Jeanne BOUCOURECHLIEV, « L'informatique face à la complexification du droit : facteur positif, négatif … ou pervers », *in Droit et informatique : L'hermine et la puce, op. cit.,* spéc. p. 41 et s. – Pierre CATALA, « Unité ou complexité », art. préc., p. 3 et s. – Patrick CHARLEMAGNE, « La complexification de la société doit-elle entraîner la complexification du droit ? », *in Droit et informatique : L'hermine et la puce, op. cit.,*. p. 21 et s.

[120] Adoption du Code de la route en 1921.

[121] René SAVATIER, « Le Droit et l'accélération de l'Histoire », *D.* 1951, chron., p. 29 et s. (« *à aucun moment, le droit ne saurait se détacher de la vie. Les transformations du film des évènements humains se projettent sur l'écran de la jurisprudence et des lois* »).

[122] V. en ce sens Christian ATIAS et Didier LINOTTE, « Le mythe de l'adaptation du droit aux faits », *D.* 1977, chron., p. 251 et s., spéc. p. 255 (« [p]*arce que l'établissement de toute solution de droit a impliqué* [des] *choix* [de faits et de buts], *l'interprète ne peut cantonner sa réflexion aux faits constatés ; il doit redécouvrir les choix initiaux, les apprécier : l'intelligence de toute règle de droit est à ce prix. Le droit ne saurait être " réduit à une science de faits "* »). – V. ég. François TERRE, *Introduction générale au droit*, 8e éd., Dalloz, coll. *Précis*, 2009, spéc. n° 40, p. 38 (« *les découvertes scientifiques, si elles appellent un encadrement juridique n'imposent pas nécessairement un alignement des règles juridiques sur les découvertes de la science, car celles-ci peuvent être bénéfiques ou maléfiques, de sorte qu'il appartient au droit, de plus en plus souvent interrogé, de prendre position* »).

servilement aux réalités. En matière d'accident de la circulation, par exemple, le législateur aurait pu adopter une position radicale en interdisant les automobiles afin de faire baisser le nombre de morts et de blessés. Cela n'a bien évidemment pas été le choix des autorités qui ont préféré élaborer un système « *tendant à l'amélioration de la situation des victimes d'accidents de la circulation et à l'accélération des procédures d'indemnisation* » [123]. De même, le développement fulgurant des capacités de traitement et de stockage des informations que l'informatique a permis, a suscité des craintes face aux menaces qui pesaient sur les données traitées. Face à ces nouveaux problèmes qui se sont posés en termes de protection des données, le législateur a dû prendre position. En adoptant la loi informatique, fichiers et libertés de 1978, il n'avait l'intention ni d'interdire la création de fichiers nominatifs ni de freiner l'utilisation de cet outil informatique mais de rechercher un « *équilibre entre les acteurs du jeu informatique* » [124], recherche qui passait nécessairement par « *la définition d'obligations et d'interdictions à l'encontre des détenteurs d'informations nominatives* » [125] et par la reconnaissance de certains droits octroyés au titulaire de ce type de données. Cet objectif est d'ailleurs clairement exprimé dès l'article 1er de la loi de 1978 qui dispose que « [l']*informatique doit être au service de chaque citoyen.* […] *Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques* » [126]. On le voit, sauf à s'enliser dans un immobilisme blâmable, le droit ne peut ignorer ces évolutions techniques et scientifiques qui posent de nouvelles problématiques juridiques auxquelles il doit se confronter sans toutefois s'incliner passivement devant de telles évolutions [127].

63. Les nouvelles technologies, un stimulant pour le droit. L'effervescence des nouvelles technologies, notamment dans les domaines de la communication et du vivant, constitue un facteur d'évolutions et d'adaptations nécessaires du droit en le conduisant à répondre aux nouvelles questions juridiques qui en découlent [128]. De nombreux exemples

[123] Loi n° 85-677 du 5 juillet 1985 tendant à l'amélioration de la situation des victimes d'accidents de la circulation et à l'accélération des procédures d'indemnisation, J.O. du 6 juillet 1985.
[124] Pierre-Alain WEILL, « État de la législation et tendances de la jurisprudence relatives à la protection des données personnelles en droit pénal français », *RID comp.* 1987-3, p. 655 et s., spéc. p. 663.
[125] Pierre-Alain WEILL, art. préc., *loc. cit.*
[126] Nathalie MALLET-POUJOL souligne que ce texte n'est pas motivé par « *un rapport de propriété qui entraverait toute utilisation de données personnelles par des tiers* » mais tend à prendre en compte « *les droits de l'individu sur ses données tout en recherchant l'équilibre entre intérêts et libertés en présence, au regard notamment du caractère privé ou sensible des informations en cause* » (« Appropriation de l'information : l'éternelle chimère », *D.* 1997, chron., p. 330 et s., spéc. n° 23).
[127] V. Michel VIVANT, « Sciences et praxis », art. préc., spéc. n° 30, p. 113 (« *Le droit est flexible, éminemment flexible. Mais il ne doit pas être infléchi en n'importe quel sens. On ne doit pas accepter cette vision instrumentale du droit* […] *qui permettrait de lui faire dire une chose et son contraire* »).
[128] COUR DE CASSATION, « L'innovation technologique appréhendée par le juge », *in L'innovation technologique,* Rapport annuel, 2005, Doc. fr., 2006, p. 59 et s. (mettant en lumière l'influence des technologies sur la propriété littéraire et artistique, le droit des marques, le droit de la concurrence, le droit bancaire, le droit pénal, le droit du travail, l'activité médicale, les risque professionnels, l'environnement). – Pour une étude plus sectorielle, v.

illustrent l'enrichissement du droit grâce à la recherche perpétuelle de solutions pertinentes et adaptées à ces nouvelles problématiques. Les NTIC ont accru la dématérialisation des échanges dans les relations personnelles, comme professionnelles. L'essor du commerce électronique a ainsi accentué le volume de documents numériques (factures, bons de commande, formulaires, conditions générales de vente, courriers électroniques …) échangés sur l'internet. Les litiges qui peuvent naître de ces relations commerciales ont mis en évidence l'importance d'assurer la sécurité juridique des transactions immatérielles en offrant aux différents intervenants la possibilité de rapporter la preuve de l'existence et du contenu de leurs accords et échanges. Pour cela, les notions d'écrit et de signature ont dû être réexaminées pour y intégrer l'écrit [129] et la signature électroniques [130] et le droit de la preuve a dû être adapté [131]. Ces nouvelles technologies induisent également des menaces : celle d'une instrumentalisation de l'homme, d'un contrôle immense que permet le fichage, la biométrie, les collecte des données, la vidéosurveillance, la géolocalisation [132]. Le traçage systématique de chaque individu conduit nécessairement à réexaminer le droit afin de prendre en compte l'ampleur de ces menaces et garantir une protection adéquate. Le système de protection des données à caractère personnel notamment, a dû être repensé pour offrir une protection à la hauteur de nouveaux risques identifiés ou pressentis. De même, les nouvelles technologies ont conduit à réfléchir sur la notion d'identité de la personne en raison de son éclatement en de multiples identités numériques [133]. En effet, à côté des éléments traditionnels d'identification que sont le nom, le prénom, la date ou encore le lieu de naissance [134], coexiste une identité numérique composée d'une multitude d'identifiants

Rafâa BEN ACHOUR et Slim LAGHMANI (sous la dir.), *Le droit international face aux nouvelles technologies*, Colloque des 11, 12 et 13 avril 2002, éd. A. Pedone, coll. *Rencontres internationales de la faculté des sciences juridiques, politiques et sociales de Tunis*, 2002. – J. FOYER, « Rapport de synthèse », *in Les nouveaux moyens de reproduction : papier, sonores, audiovisuels et informatiques, Trav. Ass. H. Capitant*, Economica, 1988, spéc. p. 17 (le droit doit « *s'adapte*[r] *sans cesse tantôt pour réfréner, tantôt pour accompagner, voire pour accélérer les conséquences des évolutions, des idées et des techniques* »).

[129] Pierre-Yves GAUTIER, « L'équivalence des supports électronique et papier au regard du contrat », *in Droit et technique – Études à la mémoire du professeur Xavier Linant de Bellefonds*, Litec – LexisNexis, coll. *Les Mélanges*, 2007, p. 195 et s.

[130] Thierry PIETTE-COUDOL, « Les errances de la signature électronique ou comment résister à la convergence de la technique et du droit », *in Droit et technique – Études à la mémoire du professeur Xavier Linant de Bellefonds*, *ibid.*, p. 395 et s.

[131] Art. 1316 et s. du C. civ. introduits par la loi n° 2001-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique, J.O. du 14 mars 2000, p. 3968 et s.

[132] Valérie LASSERRE-KIESOW, « Droit et technique », doctr. préc., spéc. n° 7.

[133] V. en ce sens, Jean FRAYSSINET, « Droit, droits et technique », art. préc., spéc. p. 4.

[134] Frédéric LESAULNIER rend compte de l'évolution des identifiants et de leur incroyable diversité. Si le nom patronymique se présente naturellement comme « *l'identifiant privilégié* » lorsque l'on évoque l'information nominative, son importance tend à s'amoindrir au regard des nombreux autres identifiants qui peuvent également concourir, même de façon indirecte, à l'identification d'une personne. L'identité de la personne peut être inscrite dans ses modes d'expression (la main, l'écriture et/ou la signature, la voix), sur son corps (la physionomie, l'apparence physique, l'empreinte digitale ou encore l'iris de l'œil de la personne), dans son corps (l'organisme humain recelant des particularités intrinsèques à chaque individu : l'examen du sang, des molécules d'ADN, les empreintes génétiques et l'odeur participent également au rôle d'identification de la personne (*L'information nominative*, Thèse sous la dir. de Pierre CATALA, Paris II, 2005, spéc. n° 31, p. 50).

numériques tels que le nom de compte d'utilisateur, le pseudonyme virtuel, l'adresse électronique, les codes d'accès, le numéro spécifique attribué à chaque ordinateur connecté à l'internet (*Internet Protocol Adress*, dit adresse IP), etc. [135], ce que le professeur Emmanuel PUTMAN résume sous le terme de « *suridentification* » [136]. Cela n'est pas sans rappeler que les technologies médicales ont, elles aussi, posé de nouvelles interrogations juridiques. Elles ont notamment conduit à reconsidérer la notion et le statut de la personne face à la possible transformation de l'humain, notamment à travers ses gênes (manipulation génétique, clonage [137]), le statut de l'embryon face à l'expérimentation et à l'utilisation de l'embryon *in vitro* [138] et à la procréation artificielle [139], mais également à s'interroger sur la brevetabilité du vivant [140]. L'ensemble de ces exemples démontrent combien le droit ne peut être réduit à un rôle d'observateur passif et doit, au contraire, faire preuve de dynamisme et de réactivité [141].

64. Les nouvelles technologies, un facteur de progrès du droit. Si l'environnement technologique vient troubler la stabilité du droit, il est également une

[135] Évoquant les évolutions que le monde virtuel a engendrées, Pierre CATALA constate que l'individu est de plus en plus réduit à des séries de numéros ou de codes à tel point qu'« [a]*ujourd'hui, toutes les données du monde intelligible sont réductibles à l'alternative manichéenne du 1 et du 0. L'ère du multimédia, qui va caractériser le siècle à venir, s'ouvre sous le signe du numéraire* » (« Le marché de l'information (aspects juridiques) », *LPA* 16 oct. 1995, n°124, p. 5 et s.).

[136] Emmanuel PUTMAN, note sous CA Saint-Denis-de-la-Réunion, 6 oct. 1989, *JCP* 1990, éd. G., II. 21504.

[137] Bronislaw KAPITANIAK et Jeanne THILLIET-PRETNAR, *Le clonage et le droit, in Science, Éthique et droit, op. cit.*, p. 319 et s.

[138] Jean-Christophe GALLOUX, « Non à l'embryon industriel. Le droit européen des brevets au secours de la bioéthique, *D.* 2009, p. 578 et s.

[139] Roberto ANDORNO, *La distinction juridique entre les personnes et les choses : À l'épreuve des procréations artificielles*, (préf. François CHABAS), tome 263, LGDJ, coll. *Bibl. dr. privé*, 1996. – CONSEIL D'ETAT, *La révision de lois de bioéthique*, Doc fr., 2009. – David SMADJA, *Bioéthique : aux sources des controverses sur l'embryon*, (préf. Jean-Marie DONEGANI), Dalloz, coll. *Nouvelle Bibliothèque de thèses*, 2009 (« *Les questions de l'IVG et de l'utilisation de l'embryon in vitro sont indifféremment rapportés à l'interrogation générale autour du statut de l'embryon* » […] « *l'absence de tout progrès et de tout changement social exclut donc par principe la question du rapport à l'embryon humain in vitro* » (*id.*, spéc p. 20).

[140] Hélène GAUMONT-PRAT, « Génie génétique, et brevetabilité du vivant : De la science au droit », « Génie génétique, et brevetabilité du vivant : De la science au droit », *in* Nicole M. LE DOUARIN (sous la dir.), *Science, éthique et droit*, (préf. Claude ALLEGRE, postface François TERRE), Odile Jacob, 2007, p. 229 et s.

[141] V. par ex. Roberto ANDORNO, *La distinction juridique entre les personnes et les choses : À l'épreuve des procréations artificielles*, *op. cit.*, spéc. n° 16, p. 7 (« *Face au défi posé par les techniques de procréation artificielle, le droit se doit aujourd'hui de préciser jusqu'où il peut accepter le processus de réduction de l'homme à son composant corporel* »). – Hélène GAUMONT-PRAT, « Génie génétique, et brevetabilité du vivant : De la science au droit », art. préc., spéc. p. 235 (« *La soumission des créations relevant des technologies nouvelles aux régimes de protection habituels suppose un ajustement de ceux-ci. L'adaptation du droit des brevets qui devait intervenir témoigne de l'évolution et de l'amélioration des mécanismes juridiques* »). – V. ég. Jean FRAYSSINET, « Droit, droits et technique », art. préc., spéc. pp. 4-5 (« *La confrontation avec les nouvelles technologies amène fréquemment à redécouvrir, à revisiter, à redessiner, des concepts et des catégories juridiques fondamentaux* […]. *Le juriste doit revenir à l'essence, au sens premier des notions et catégories pour les rendre applicables à l'environnement nouveau induit par les technologies* […]. *Il en va ainsi pour les notions de personne, l'identité, la propriété, la vie privée, la distinction entre l'espace public et l'espace privé, la responsabilité, la sécurité, le contrat, le principe de précaution, les procédures. Le paysage juridique peut s'en trouver modifier* »). – Sur le dynamisme du droit, v. ég. Michel VIVANT, « Sciences et praxis », art. préc., spéc. n° 8, p. 110 (« *C'est bien de fantasme qu'il s'agit : celui qui consiste à rêver, à imaginer, à croire en un droit immuable, gravé une fois pour toutes dans la pierre,qui aurait dit à jamais une vérité que rien ne pourrait atteindre, qui figerait ainsi les choses, mentalités et comportements* »).

opportunité de le faire progresser [142] en lui donnant l'occasion de relever les défis que les nouvelles technologies lui lancent et les conflits d'intérêts qu'elles lui imposent d'arbitrer. La confrontation du droit positif à cet environnement technologique conduira à constater la précarité de certaines constructions juridiques traditionnelles et encouragera le juriste à repenser le droit pour parvenir à maîtriser ces évolutions technologiques [143]. Pour cela, il devra faire preuve d'une certaine souplesse dans son analyse critique, adopter une « ouverture d'esprit » [144]. En effet, la complexité des phénomènes invite à décloisonner les différentes branches et disciplines juridiques pour les croiser et adopter ainsi une approche transversale, multidisciplinaire. À cet égard, le *spamming* illustrera la démarche que doit adopter un juriste confronté à ces phénomènes technologiques. La diversité des formes de *spamming* ne peut se satisfaire d'une réponse unique, le juriste devra en effet puiser dans différents droits pour répondre au mieux aux problématiques posées. Ainsi, plutôt que d'envisager les champs « droit » et « technique » sur le registre de l'opposition, comme deux mondes totalement hermétiques, il convient, de façon plus pertinente, de les examiner comme deux champs complémentaires ayant une influence réciproque [145]. Enfin en pratique, on observe, sous l'influence des techniques, l'émergence de nouvelles disciplines juridiques telles que le droit des nouvelles technologies de la communication et de l'information, de la santé et des biotechnologies. La multiplication des enseignements, de plus en plus pointus, se traduit à son tour par l'apparition de juristes spécialisés, capables de répondre à des problématiques présentant, au-delà des aspects purement juridiques, une coloration technique prononcée [146]. De même, apparaissent, au sein des juridictions, des chambres spécialisées composées de magistrats spécialisés. Cette évolution témoigne de la technicité croissante des débats judiciaires qui nécessite le plus souvent le recours à un expert. Cette réactivité du droit se manifeste encore par l'émergence d'autorités administratives indépendantes, comme

[142] S'interrogeant sur le progrès du droit, Gilles LEBRETON constate que « [l]*e progrès du droit est fragile. Rien n'est jamais définitivement acquis. Reflet de la conscience collective, le droit est voué à se transformer au gré de ses évolutions. Paraphrasant Chateaubriand, on pourrait dire qu'il en va des règles juridiques comme des nations : elles " marchent à leur destinée. Comme certaines ombres de Dante, il leur ait impossible de s'arrêter "* » (« Y-t-il un progrès du droit, *D.* 1991, chron., p. 99 et s., spéc. p. 104).

[143] Jérôme HUET observait déjà que « *l'informatique, et ses prolongements, peuvent accroître la rationalité dans la maîtrise de la règle de droit*. […] [O]*n perçoit qu'il y aurait beaucoup de progrès à faire et que les techniques de traitement de l'information devraient permettre d'améliorer notre maîtrise des notions juridiques et de la terminologie* » (Jérôme HUET, « Droit, informatique et rationalité », art. préc., spéc. p. 85).

[144] Jean FRAYSSINET, « Droit, droits et technique », art. préc.

[145] Hélène GAUMONT-PRAT, « Génie génétique, et brevetabilité du vivant : De la science au droit », art. préc., spéc. p. 241 (« *le droit s'enrichit au contact du progrès technique et scientifique, il est modernisé, mais le droit influence également les sciences et les techniques car il a pour mission leur régulation* »).

[146] Pierre CATALA, « Unité ou complexité », art. préc. spéc. pp. 3-4. – V. ég. Jean FRAYSSINET, « Droit, droits et technique », art. préc., spéc. p. 6 (« *ainsi des praticiens, de plus en plus spécialisés, conjuguent leurs efforts comme dans une espèce de polyclinique pour ne pas dire de CHU de la pathologie juridique* »).

la CNIL, chargées de réguler les effets des principales évolutions technologiques sur la société [147].

65. L'internet, une mise en perspective du droit selon de nouvelles références spatiales. Les NTIC, en particulier l'internet, ignorent les frontières. Le droit qui se met en place autour d'elles ne peut être conçu exclusivement dans un cadre national ou du moins, en ignorant les ressources et approches des différents systèmes juridiques. Les phénomènes qui ont émergé de l'internet notamment, produisent des effets, par nature, extraterritoriaux [148]. Le *spamming* est à cet égard une bonne illustration puisque dans la plupart des cas, les *spams*, envoyés depuis un territoire seront adressés à des milliers, voire des millions de destinataires localisés dans différents pays. La dispersion géographique du *spamming* risque, en cas de poursuites judiciaires engagées contre le « spammeur », de faire intervenir plusieurs juridictions nationales et plusieurs lois nationales. L'application automatique et autoritaire de notre droit national encourt dès lors un fort risque d'échec dans la mesure où il pourra être purement et simplement ignoré par les autres pays. Toute analyse s'attachant à un phénomène international nécessite donc de s'intéresser aux droits des pays étrangers et de tenir compte des éventuelles oppositions entre États que pourraient générer le différend. Les situations qui naissent sur l'internet imposent de s'ouvrir aux autres droits. Cette démarche est du reste particulièrement fertile puisque notre droit interne pourrait, de cette façon, s'enrichir des expériences étrangères et sans doute parvenir à combler les lacunes persistantes.

§ 3. LA METHODE DE LA RECHERCHE

66. Pour mener à bien notre recherche, nous avons adopté une démarche générale qui oriente la construction et la structuration de notre raisonnement (A.) tout en y associant une démarche de droit comparé, indispensable lorsque nous envisageons d'étudier un

[147] Jean FRAYSSINET, « Droit, droits et technique », art. préc., *loc. cit.*

[148] Slim LAGHMANI, « Le droit international face aux nouvelles technologies, rapport introductif », *in* Rafâa BEN ACHOUR et Slim LAGHMANI (sous la dir.), *Le droit international face aux nouvelles technologies*, Colloque des 11, 12 et 13 avril 2002, éd. A. Pedone, coll. *Rencontres internationales de la faculté des sciences juridiques, politiques et sociales de Tunis*, 2002, spéc. pp. 30-31 (« *Les innovations technologiques sont, à la fois, causes et effets de l'ouverture du Monde. Le formidable développement des techniques de télécommunications, des satellites, des réseaux informatiques a permis l'accélération du processus de la mondialisation, mais, en retour, les problèmes posés par les innovations technologiques sont également mondiaux dans les deux sens, d'abord, en ce qu'ils ignorent les frontières, ensuite en ce sens que la libre circulation des biens et des personnes fait qu'il ne sert à rien de régler certains problèmes à l'échelle nationale ou même régionale. Font partie de la première catégorie, les problèmes posés par les réseaux informatiques ou les risques engendrés par le nucléaire. Ainsi, la cybercriminalité ou le commerce électronique sont par définition des phénomènes transnationaux. De même, le risque nucléaire, on en a fait l'expérience avec Tchernobyl, ignore les frontières. Font partie de la seconde catégorie les problèmes posés par les biotechnologies* »).

phénomène qui a vocation à évoluer dans un espace dénué de toutes frontières géographiques (B.).

A. LA DEMARCHE GENERALE

67. Les lois spéciales désignent celles qui « *donnent une règle particulière à une série de cas déterminés* » [149]. Elles sont créées ponctuellement pour répondre à des besoins économiques et sociaux particuliers, par opposition aux lois générales « *qui déterminent les règles applicables à tous les cas qui composent un genre donné de rapports juridiques* » [150]. Loi spéciale et loi générale apparaissent, on le voit, comme dépendantes l'une de l'autre, elles sont liées par « *un rapport d'espèce à genre* » [151]. Cette opposition entre le spécial et le général est familière aux juristes [152], elle « *fait presque figure de réflexe naturel* » [153]. Cette bipartition se retrouve dans de nombreuses disciplines juridiques : par exemple, en droit pénal [154], en droit des contrats [155], en droit des sociétés [156], en droit de la responsabilité civile[157], en droit international privé [158].

[149] Raymond GASSIN, « Lois spéciales et droit commun », *D.* 1961, chron., p. 91 et s., spéc. n° 1, p. 91.

[150] *Id., loc. cit.*(« *Constituent ainsi des lois spéciales les art. 1384 à 1386 du c. civ. en ce qu'ils posent des règles particulières du fait des choses et du fait d'autrui, tandis que les art. 1382 et 1383 sont la loi générale en matière de responsabilité civile* »).

[151] *Id., loc. cit.* – Cette interaction entre ces deux termes apparaît dans les définitions données par le *Vocabulaire juridique* de l'Association Capitant : est commun ce « [q]*ui s'applique à toutes les espèces d'un genre, par opposition à spécial à particulier* » ou, dans un autre sens, ce « *qui s'applique en principe (sauf exceptions) à toutes les personnes et à toutes les affaires par opposition à exceptionnel* », ce qui est « *résiduellement applicable à tous les cas non exceptés* » ; est spécial ce « *qui ne concerne qu'un ensemble des cas abstraitement défini mais constituant une espèce assez étroite* […] *par opposition à un genre plus étendu régi par une règle générale* » ou « [d]*ans un sens voisin,* [ce] *qui est propre à une espèce d'acte ou de fait, par opposition à ce qui est commun à toutes les espèces du genre* » (Gérard CORNU, *Vocabulaire juridique*, Ass. H. CAPITANT, 8e éd., Quadridge-PUF, 2007, v. « commun » et v. « spécial »).

[152] Sur la dialectique du spécial et du général, v. notamment Jean-Pascal CHAZAL, « Réflexions épistémologiques sur le droit commun et les droits spéciaux », *in* Christophe ALBIGES, Jean-François ARTZ, Juan-Manuel BADENAS CARPIO et al., *Études du droit de la consommation, Liber Amicorum Jean CALAIS-AULOY*, Dalloz, coll. *Mélanges*, 2004, p. 279 et s. – Raymond GASSIN, « Lois spéciales et droit commun », chron. préc. – Denis MAZEAUD, « L'imbrication du droit commun et des droits spéciaux », *in* Geneviève PIGNARRE (sous la dir.), *Forces subversives et forces créatrices en droit des obligations* : *Rétrospective et perspectives à l'heure du Bicentenaire du code civil*, Dalloz, 2005, p. 73 et s. – Frédéric POLLAUD-DULIAN, « Du droit commun au droit spécial – et retour », *in Aspects actuels du droit des affaires, Mélanges en l'honneur de Yves Guyon*, Dalloz, 2003, p. 925 et s. – Bernard SAINTOURENS, *Essai sur la méthode législative : droit commun et droit spécial*, thèse sous la dir. de Jean DERRUPE, Bordeaux I, 1986. – Laurent LEVENEUR, « Le Code civil, cadre normatif concurrencé », *in* Bernard SAINTOURENS (sous la dir.), *Le Code civil, une leçon de légistique ?*, Economica, coll. *Études juridiques*, 2006, p. 123 et s.

[153] Charlotte GOLDIE-GENICON, *Contribution à l'étude des rapports entre le droit commun et le droit spécial des contrats*, (préf. Yves LEQUETTE), tome 509, LGDJ, coll. *Bibl. dr. privé*, 2009, spéc. n° 10.

[154] Le cas en droit pénal qui se divise entre le droit pénal général qui regroupe les règles communes à l'ensemble des infractions (v. par ex. Frédéric DESPORTES et Francis LE GUNEHEC, *Droit pénal général*, 16e éd., Economica, coll. *Corpus Droit privé*, 2009. – Jean PRADEL, *Droit pénal général*, 18e éd., Cujas, coll. *Référence*, 2010), et le droit spécial qui traite des infractions et précise pour chacune d'entre elles leurs éléments constitutifs, les peines et le cas échant, les spécificités de la poursuite et de la sanction (v. par ex. Jean PRADEL et Michel DANTI-JUAN,

68. Cette dialectique constitue « *une véritable balise de la méthodologie juridique* » [159] pour procéder à un examen critique des solutions propres à telle ou telle problématique. Dans le cadre de notre recherche, l'avènement d'une ère dominée par l'informatique a suscité au sein de la société dans son ensemble un besoin grandissant de contrôler l'informatique afin d'éviter les dérives pressenties au regard des capacités inouïes qu'elle offrait en matière de traitement des informations [160]. La crainte que l'outil informatique se développe au mépris de la protection des libertés publiques a très tôt incité les législateurs européens à adopter une législation relative à la protection des données à caractère personnel [161]. En France, la loi informatique, fichiers et libertés est venue encadrer le traitement informatique de ce type de données [162] afin de répondre à cet impératif. Par ailleurs, l'internet qui est apparu comme un média de communication extrêmement précieux pour la prospection commerciale, a permis à certains esprits malveillants de l'utiliser pour commettre des actes illicites dont le *spamming* est une illustration patente. La méfiance croissante des internautes envers l'internet et le commerce électronique a ainsi encouragé le législateur à adopter la loi pour la confiance dans l'économie numérique, destinée

Droit pénal spécial, 5e éd., Cujas, coll. *Référence*, 2010. – Michel VERON, *Droit pénal spécial*, 13e éd., Dalloz-Sirey, coll. *Sirey Université*, 2010).

155 « *Le droit commun des contrats dessine la charpente du droit des contrats, son squelette ; il détermine les traits communs du genre contractuel, le patrimoine commun partagé par tous les contrats. Il est, en somme le modèle au regard duquel se construisent les régimes applicables aux différents contrats* » (Charlotte GOLDIE-GENICON, *Contribution à l'étude des rapports entre le droit commun et le droit spécial des contrats*, (préf. Yves LEQUETTE), tome 509, LGDJ, coll. *Bibliothèque de droit privé*, 2009, spéc. n° 108, p. 151 (« [l]*e droit commun des contrats a précisément pour fonction d'assurer ce minimum d'unité entre les différents contrats qui permet de reconnaître dans chacune des différentes espèces contractuelles les traits d'une même famille* »).

156 Le droit des sociétés se scinde en deux types de dispositions : les règles communes à toutes les sociétés et celles spécifiques à certaines sociétés.

157 En droit de la responsabilité civile, coexistent des régimes généraux et des régimes spéciaux de responsabilité (v. par ex. Geneviève VINEY, *Introduction à la responsabilité : évolution générale, responsabilité civile et responsabilité pénale, responsabilité contractuelle et responsabilité délictuelle*, (sous la dir. de Jacques GHESTIN), 2e éd., L.G.D.J., 1995, spéc. p. 452 (« *la distinction entre responsabilité contractuelle et délictuelle est appelée à perdre de son importance au profit d'une autre distinction, qui tend à s'affirmer aujourd'hui de plus en plus entre le " droit général " et les régimes spéciaux de responsabilité civile* »).

158 Le droit international privé général traite de l'ensemble des questions relatives aux conflits de juridictions et de lois alors que le droit international spécial réunit les applications concrètes du droit international privé (question de la compétence juridictionnelle et législative, reconnaissance des décisions rendues, …) dans des divers domaines (v. par ex. Dominique BUREAU et Horatia MUIR WATT, *Droit international privé*, tome 1 (Partie générale), 2e éd., PUF, coll. *Thémis Droit*, 2010 et tome 2 (Partie spéciale), 2e éd., PUF, coll. *Thémis Droit*, 2010 (cette partie traitant de l'application du droit international privé dans trois sphères distinctes : personnelle, familiale et économique).

159 Charlotte GOLDIE-GENICON, *Contribution à l'étude des rapports entre le droit commun et le droit spécial des contrats*, *op. cit.*, spéc. n° 11).

160 Dans les années 70, la révélation publique en France du projet d'élaboration d'un « Système Automatisé pour les Fichiers Administratifs et le Répertoire des Individus», connu sous l'acronyme « SAFARI », qui prévoyait la mise en place d'un identifiant unique (numéro de sécurité sociale) pour interconnecter les fichiers publics a soulevé de vives inquiétudes (sur le système SAFARI, v. Philippe BOUCHER, « Safari ou la chasse aux français », Le Monde, 21 mars 1974, p. 9, disponible sur : http://rewriting.net/wp-content/le_monde_-_21_03_1974_009-3.jpg).

161 Sur les risques de l'informatique, v. ég. Guy BRAIBANT, *Données personnelles et société de l'information : Transposition en droit français de la directive 95/46*, Rapport au Premier ministre, Doc. fr., coll. *Rapports officiels*, Paris, 1998, spéc. p. 6.

162 André VITALIS, *Informatique, Pouvoir et Libertés*, (préf. Jacques ELLUL), 2e éd., Economica, coll. *Politique comparée*, Paris, 1988, spéc. p. 135 et s.).

notamment à fixer une réglementation stricte en matière d'envois commerciaux [163]. L'analyse de la loi anti-*spam* française est donc particulièrement importante puisque selon le classement trimestriel réalisé par SOPHOS des douze principaux pays relayeurs de *spam*, il ressort que pour la période d'octobre à décembre 2010, la France occupe le deuxième rang des pays européens relayeurs de *spams* avec 3,45%, devancée par le Royaume-Uni avec 4,54% [164].

69. Pour mener à bien notre recherche, nous débuterons ainsi notre analyse en interrogeant la loi IFL et la LCEN afin de déterminer dans quelle mesure ces lois pourront s'imposer comme un fondement d'action efficace pour les « spammés ». L'examen des solutions offertes par ces deux lois spéciales pour lutter contre le *spamming* révèlera leurs imperfections et leur incapacité à assurer une protection pleinement satisfaisante pour les « spammés », leur champ d'application étant, par nature, limité [165]. Pour pallier ces carences, nous nous tournerons vers le droit commun qui a toujours une vocation subsidiaire à intervenir dès l'instant où que les dispositions spéciales ne l'évincent pas [166]. La question de l'apport du droit commun à telle ou telle discipline juridique est en effet une problématique classique dès lors que le droit spécial risque de n'apporter que des réponses incomplètes au différend [167], ce qui est particulièrement le cas en présence de nouvelles technologies. Ainsi, droit spécial et droit commun entretiennent nécessairement des liens étroits et nombre de travaux doctrinaux ont examiné et réfléchi sur les relations qui pouvaient exister entre le droit commun des obligations et le droit du travail [168], le droit de la consommation [169], le

[163] Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.
[164] SOPHOS, " The top twelve spam relaying countries for October – December 2010 ", 11 janv. 2011, disponible sur : http://www.sophos.com/en-us/press-office/press-releases/2011/01/dirty-dozen-q42010.aspx.
[165] Frédéric POLLAUD-DULIAN, « Du droit commun au droit spécial – et retour », art. préc., spéc. p. 940.
[166] sur cette fonction du droit commun, v. Christophe RADE, *Droit du travail et responsabilité civile*, (préf. Jean HAUSER), LGDJ, coll. *Bibl. dr. privé*, tome 282, 1997, spéc. n° 249, p. 157 (« *Le droit civil occupe au sein de la famille du droit privé une place de choix, celle de droit commun autour duquel gravitent les autres disciplines.* […] *le droit commun a vocation à s'appliquer de manière supplétive toutes les fois qu'une loi spéciale n'en dispose pas autrement* »))
[167] V. par ex. G.-H. CAMERLYNCK, « L'autonomie du droit du travail », *D.* 1956, chron., p. 23 et s. – Gérard LYON-CAEN, « Du rôle des principes généraux du droit civil en droit du travail (première approche) », *RTD civ.* 1974, p. 229 et s. – Marie-Noël JOBARD-BACHELLIER et Vincent BREMOND, « De l'utilité du droit de la responsabilité pour assurer l'équilibre des intérêts des contractants (à propos des rapports entre droit commun et droit du cautionnement), *RTD* com. 1999, p. 327 et s. – Jean-Pierre PIZZIO, « La protection du consommateur par le droit commun des obligations », *RTD* com. 1998, p. 53 et s. (« *La protection de la partie la plus faible, qu'elle ait la qualité de consommateur ou non, est devenue un objectif commun au droit de la consommation et au droit des obligations rénové par une jurisprudence créatrice. […] Le droit commun reste en effet présent à double titre, d'une part, il a vocation naturelle à combler les insuffisances du droit de la consommation, c'est son domaine réservé et d'autre part, sous l'effet d'une jurisprudence qui le vivifie, il concurrence de plus en plus le droit de la consommation sur ses propres terres, c'est le domaine partagé* » (*id.*, spéc. n° 8, p. 57).
[168] Jean-Jacques DUPEYROUX, « Droit civil et droit du travail : l'impasse », *Dr. soc.* 1988, p. 371 et s. – Gérard LYON-CAEN, « Du rôle des principes généraux du droit civil en droit du travail », art. préc. – Jean PELISSIER, « Droit civil et contrat individuel de travail », *Dr. soc.* 1988, p. 387 et s. – Christophe RADE, *Droit du travail et responsabilité civile*, *op. cit.*, spéc. n° 543, p. 343 (« *L'analyse des rapports entre la responsabilité civile et le droit du travail permet de mettre en évidence les insuffisances, voire les incohérences des règles propres aux*

droit de la concurrence [170], le droit de la propriété intellectuelle [171], le droit des procédures collectives [172] ou encore le droit des sociétés [173]. L'une de ses fonctions premières est en effet de fournir une réponse aux insuffisances de la loi spéciale [174] et de combler les lacunes constatées. Il reste alors à préciser ce qu'il convient d'entendre par « droit commun ». La question mérite réflexion en raison de l'imprécision de la notion même de droit commun. Le droit civil se voit traditionnellement attribuer le rôle de droit commun des rapports privés [175], par opposition aux règles ne régissant que certaines relations particulières. Toutefois, il est essentiel de garder à l'esprit que le rapport entre le droit spécial et le droit commun présente

relations professionnelles. […] *La responsabilité civile agit alors comme un révélateur puisqu'elle intervient lorsque le droit spécial se retire* »).

[169] Georges BERLIOZ, « Droit de la consommation et droit des contrats », *JCP* 1979, éd. G., I. 2954. – Michel BORYSEWICZ, « Les règles protectrices du consommateur et le droit commun des contrats : Réflexions à propos de la loi n° 78-23 du 10 janvier 1978 sur la protection de l'information des consommateurs de produits et de services », *in Études offertes à Pierre KAYSER*, (préf. Charles DESBBASH), tome 1, PUF, 1979, p. 91 et s. – Jean CALAIS-AULAIS, « L'influence du droit de la consommation sur le droit civil des contrats », *RTD civ*. 1994, p. 239 et s. – Nicole CHARDIN, *Le contrat de consommation de crédit et l'autonomie de la volonté*, LGDJ, 1998. – Jean-Pierre PIZZIO, « La protection des consommateurs par le droit commun des obligations », art. préc..

[170] Frédérique DREIFUSS-NETTER, « Droit de la concurrence et droit commun des obligations », *RTD civ*. 1990, p. 369 et s. – Marie MALAURIE-VIGNAL, « Droit de la concurrence et droit des contrats », *D.* 1995, chron., p. 51 et s. (« *L'étude des rapports entre le droit civil et le droit de la concurrence est marquée par l'harmonie et le conflit* » (*id.*, spéc. p. 51). – Sur la question de la convergence du droit du marché et du droit des obligations, v. Nicole DECOOPMAN, « Droit du marché et droit des obligations », *in Le renouvellement des sources du droit des obligations*, tome 1/Lille-1996, LGDJ, Ass. H. Capitant, 1996, p. 141 et s. – Yves SERRA, « Les fondements et le régime de l'obligation de non-concurrence », *RTD com.* 1998, p. 7 et s.

[171] Jean-Michel BRUGUIERE, Nathalie MALLET-POUJOL et Agnès ROBIN (sous la dir.), *Propriété intellectuelle et droit commun*, P.U.A.M., coll. *Institut de droit des affaires*, 2007.

[172] V. par ex. Yves GUYON, « Le droit des contrats à l'épreuve du droit des procédures collectives », *in Le contrat au début du XXI^e siècle, Études offertes à Jacques GHESTIN*, L.G.D.J., 2001, p. 405 et s. – Marie-Hélène MONSERIE, « Aperçu sur les rapports récents de la confrontation du droit des procédures collectives et du droit des obligations », *in Prospectives du droit économique, Dialogues avec Michel JEANTIN*, (préf. Jean CARBONNIER), Dalloz, 1999, p. 429 et s.

[173] Jean-Pierre BERTREL, « Liberté contractuelle et sociétés : Essai d'une théorie du " juste milieu " en droit des sociétés », *RTD com*. 1996, p. 595 et s. – Michel JEANTIN, « Droit des obligations et droit des sociétés », *in Mélanges Laurent BOYER*, Presse universitaire des Sc. Soc. de Toulouse I, 1996, p. 317 et s., spéc. p. 331 (« *Moins encore que jadis, le droit des sociétés ne peut être réellement compris que grâce à une référence constante au droit des obligations qui en constitue non seulement le fondement, mais encore la sève qui irrigue les rameaux, jusqu'au plus éloigné* »).

[174] Denis MAZEAUD, « L'imbrication du droit commun et des droits spéciaux », art. préc., spéc. n° 13, p. 80 (« *Le droit commun qui s'incarne dans une loi ne suffit pas toujours … même ; ils comportent des imprécisions, des lacunes, des failles, des imperfections qui l'empêchent de régir intégralement ou efficacement les situations qui entrent dans son champ d'application* »).

[175] Sur la reconnaissance du droit civil comme droit commun, v. par ex. Jean-Luc AUBERT et Éric SAVAUX, *Introduction au droit et thèmes fondamentaux du droit civil*, 13^e éd., Sirey, 2010, spéc. n° 49, p. 37 (« *Le droit civil, qui a longtemps été le droit commun français* […] *reste encore aujourd'hui une sorte de droit commun privé. En effet lorsque, dans un domaine relevant normalement du droit commercial ou d'un droit mixte, naît un litige de nature privée, et qu'il existe, pour le résoudre, aucune règle spéciale, c'est aux principes et aux techniques du droit civil qu'il convient de se référer pour trancher* »). – Jean-Louis BERGEL, *Méthodologie juridique*, 1re éd., P.U.F., coll. *Thémis droit privé*, 2001, spéc. p. 191. – Jean CARBONNIER, *Droit civil : Les obligations*, tome 4, 22^e éd. refondue, P.U.F., coll. *Thémis droit privé*, 2000, spéc. n° 3, p. 18 (« [l]*e droit civil* […] *a valeur de droit commun* »). – Philippe MALAURIE, Patrick MORVAN, *Introduction générale*, 3^e éd., Defrénois, 2009, spéc. n° 64, p. 53 et s. – Bernard SAINTOURENS, *Essai sur la méthode législative : droit commun et droit spécial*, thèse préc., spéc. n° 34, p. 71 et n° 135 et s., p. 191 et s. – V. pour une position plus nuancée, Jean-Pascal CHAZAL, qui énonce que « *le Code civil est davantage un droit premier, directeur et général qu'un véritable droit commun. En quelque sorte, il n'est droit commun que par synecdoque, à cause des règles générales qu'il contient* » (« Réflexions épistémologiques sur le droit commun et les droits spéciaux », art. préc., spéc. p. 285).

une certaine relativité [176] puisque certaines des dispositions du Code civil pourront elles-mêmes constituer le droit commun lorsqu'elles ont vocation à intervenir dans un domaine limité. Tout dépend donc du champ de référence considéré. Par exemple, si l'article 1384 alinéa 1er du Code civil constitue une « [l]*oi spéciale au regard de l'art. 1382, l'art. 1384, § 1er, qui, selon la jurisprudence édicte une règle générale de responsabilité du fait des choses, fait figure de loi générale à côté de l'art. 1385 sur la responsabilité du fait des animaux et de l'art. 1386 qui ne concerne que la responsabilité des dommages causés par la ruine des bâtiments* ») [177]. Il convient dès lors d'admettre que le droit civil ne peut constituer un droit commun dans l'absolu et que la notion de droit commun ne peut être définie que par référence à un secteur particulier [178] : ne parle-t-on pas en effet du « droit commun de la vente » [179], du « droit commun du travail » [180], ou encore de « droit commun du cautionnement » [181] alors même que les dispositions édictées sont spéciales si on les compare à des règles de portée générale ? En reconnaissant que le droit commun ne peut être saisi que par rapport à un référentiel spécifique, l'« ambiguïté » [182] de la notion de droit commun semble alors disparaître. Il ne s'agit pas en effet d'analyser le droit commun en général mais celui qui a vocation à encadrer la pratique du *spamming* par opposition aux lois spéciales (loi relative à la protection des données à caractère personnel et celle encadrant spécifiquement le *spamming*). Autrement dit, le droit commun doit être entendu comme celui régissant les cas de *spamming* autres que ceux couverts pas les lois spéciales. Il reste alors à déterminer

[176] Raymond GASSIN, « Lois spéciales et droit commun », chron. préc., spéc. n° 1, p. 91. – Sur le caractère relatif de la notion de droit commun, v. ég. Jean-Louis BERGEL, *Méthodologie juridique, op. cit.*, spéc. p. 192. – Frédéric POLLAUD-DULIAN, « Du droit commun au droit spécial – et retour », art. préc., spéc. p. 936 (« *en fonction de la question posée, le droit commun peut se révéler dans les règles de droit spécial par rapport à un droit encore plus spécial* ». – Bernard SAINTOURENS, *Essai sur la méthode législative : droit commun et droit spécial*, thèse préc., spéc. n° 11 et n° 28.

[177] Sur le caractère relatif de cette opposition, v. Raymond GASSIN, « Lois spéciales et droit commun », chron. préc., spéc. n° 1, p. 91 (pour saisir cette relativité du rapport entre ces deux termes, il donne un exemple très éclairant :

[178] V. en ce sens Charlotte GOLDIE-GENICON, *Contribution à l'étude des rapports entre le droit commun et le droit spécial des contrats, op. cit.*, (« *Le droit commun n'a de sens que par rapport au référentiel choisi, qu'il s'agisse d'un territoire, d'une matière ou plus modestement d'un contrat particulier* »). – Pour un exemple en droit du travail, v. Christophe RADE, *Droit du travail et responsabilité civile, op.cit.*, spéc. n° 543, p. 343 (Le droit du travail a « *vocation à devenir le droit commun du secteur particulier de l'activité humaine qu'*[il] *régit* »).

[179] Philippe MALAURIE et Laurent AYNES, *Cours de droit civil : Les contrats spéciaux*, 14e éd., Cujas, 2001, spéc. n° 167, p. 147 (« *La vente aux enchères publiques peut être " volontaires " ; elle est alors faite devant un notaire. Elle relève davantage du droit commun de la vente, puisque le cahier des charges est alors l'œuvre du vendeur* »). – Cass. civ. 3e, 26 mai 1994, pourvoi n° 92-15911, *Bull. civ.* III, n° 110 (Le vendeur d'un appartement en l'état futur d'achèvement à construire est débiteur comme dans le droit commun de la vente d'une obligation de délivrance).

[180] V. par ex. Elsa PESKINE, *Réseaux d'entreprises et du droit du travail*, (préf. Antoine LYON-CAEN), LGDJ, coll. *Bibl. dr. social*, tome 45, 2008, spéc. nos 394-396, pp. 217-218.

[181] Dominique LEGEAIS, « Le Code la consommation siège d'un nouveau droit commun du cautionnement : Commentaires des dispositions relatives au cautionnement introduites par les loi du 1er août 2003 relatives à l'initiative économique et sur la ville », *JCP* 2003, éd. E., 1433, p. 1610 et s. – Yves PICOD, « Sanction du principe de proportionnalité en droit commun du cautionnement », *D.* 2004, chron., p. 204 et s.

[182] Jean-Pascal CHAZAL, « Réflexions épistémologiques sur le droit commun et les droits spéciaux », art. préc., spéc. p. 281 (signalant le caractère « équivoque » de la notion de droit commun et décrit les « mutations sémantiques » qu'elle a suivies).

précisément sur quel droit commun portera notre analyse. Pour les besoins de notre recherche, le recours au droit commun est, rappelons-le, destiné à renforcer la protection des « spammés ». Cet objectif correspond en réalité à deux objectifs distincts puisqu'il conviendra non seulement de sanctionner les divers cas de *spamming* mais également d'assurer une indemnisation de l'ensemble des « spammés ». Dans cette double perspective, nous ferons appel d'une part au droit pénal et d'autre part au droit commun de la responsabilité civile [183] ; l'un et l'autre jouant un rôle de droit commun au regard de l'objectif propre pour lequel ils ont vocation à intervenir (objectif de sanction et objectif d'indemnisation). Dans cette hypothèse, il n'existe pas de conflits entre ces deux branches du droit commun, l'un et l'autre pouvant coexister dans la mesure où ils poursuivent des objectifs propres (sanction/réparation) mais dans un but final commun : le perfectionnement du droit. Dans cette optique de perfectionnement du droit, il conviendra également, sous un regard critique, de déterminer si les solutions du droit commun apparaissent pleinement satisfaisantes et à défaut, de proposer, à titre prospectif, les évolutions ou adaptations qu'il conviendrait d'envisager.

B. LA DEMARCHE DE DROIT COMPARE

70. Nous avons souligné à plusieurs reprises que le *spamming* était une pratique, par nature, internationale. Dans ces conditions, il nous est apparu indispensable de ne pas limiter notre étude au seul droit français. Tout juriste confronté à un phénomène dont les effets dépassent les frontières d'un pays doit, pour bien conseiller, avoir nécessairement le souci de s'informer de ce qui est fait au-delà de ses frontières [184].

71. Les fonctions du droit comparé. Lorsque l'on envisage une étude de droit comparé, il apparaît naturel de s'interroger au préalable sur les objectifs du droit comparé et la manière de les atteindre.

[183] Frédéric POLLAUD-DULIAN observant à ce titre qu' « *il est bien difficile de faire jouer au droit civil un rôle de droit commun à l'égard du droit pénal* […] et que] *le droit pénal joue lui-même un rôle de droit commun à l'égard de toute une série de matière spécialisées qui en découlent. Ainsi, force est d'admettre qu'il peut y avoir plusieurs droits communs qui coexistent* » (Du droit commun au droit spécial – et retour », art. préc., spéc. pp. 936-937).

[184] Georges FLECHEUX, « La situation juridique en France : Le point de vue des professions juridiques », *in Le droit comparé aujourd'hui et demain, op. cit.,* spéc. p. 61 et s. (« *Le droit comparé est entré dans la vie des avocats et du juge. Il devient de plus en plus difficile d'imaginer que les juristes français puissent tenir une place sur le " marché du droit " en Europe en restant indifférents à la pratique du droit étranger dans la seule contemplation des dispositions nationales* » (*id.*, spéc. p. 62).

72. La fonction première du droit comparé est d'enrichir et d'améliorer la connaissance du droit, de son droit national mais aussi des droits étrangers [185]. Cette première fonction appelle dès à présent une remarque importante qui consiste à distinguer l'approche du droit comparé de l'étude des droits étrangers. Si la comparaison implique sans conteste l'observation des droits étrangers, elle ne peut se réduire à cette seule mission [186]. La démarche se révèle plus exigeante [187]. « *Le droit comparé est en effet essentiellement comparatif en ce qu'il ne décrit pas un droit étranger pour lui-même, mais toujours par rapport à un autre droit* » [188]. Cet exercice de comparaison permet au moyen de la confrontation de deux ou plusieurs systèmes juridiques de distinguer ce qui est original de ce qui est commun [189], d'identifier les ressemblances et les différences, puis d'en apprécier l'étendue et les conséquences qui en découlent [190]. Pour cela, nous avons procédé à l'analyse d'un autre système de droit étranger que notre système national afin de mieux connaître et comprendre les deux. Toutefois, comme nous venons de l'expliquer, l'acquisition de la connaissance et du savoir que permet une étude de droit comparé ne se réduit pas à la seule observation de deux systèmes juridiques. Cet exercice de comparaison sera également destiné à mettre en perspective ces deux systèmes juridiques afin de comprendre les faiblesses et les imperfections de chacun.

---

[185] Gino GORLA, « Intérêts et problèmes de la comparaison entre le droit continental et la Common law », *RIDC* 1963, p. 5 et s., spéc. p. 6 et s. – Étienne PICARD, « L'état du droit comparé en France, en 1999 », *RIDC* 1999, p. 885 et s. (« *Le droit comparé constitue* […] *cette discipline scientifique cherchant à connaître et surtout – à ce quoi, néanmoins, il ne tend pas toujours assez, en fait – à comprendre les droits étrangers* » (*id.*, p. 887).

[186] Rodolfo SACCO, *La comparaison juridique au service de la connaissance du droit*, Economica, coll. *Études juridiques comparatives*, 1991, p. 8 et s., spéc. p. 8 (« *La comparaison suppose évidemment l'observation de plusieurs modèles juridiques, mais elle dépasse cette simple observation* »). – Étienne PICARD, « L'état du droit comparé en France, en 1999 », art. préc., spéc. p. 887 (« *Le droit comparé constitue* […] *cette discipline scientifique cherchant à connaître et surtout – à ce quoi, néanmoins, il ne tend pas toujours assez, en fait – à comprendre les droits étrangers* ».

[187] Pierre LEGRAND, « Comparer », *in* Jacques Robert, Rodlofo Sacco, Pierre Legrand et al., *Le droit comparé aujourd'hui et demain : Colloque du 1er décembre 1995, Paris*, Société de législation comparée, 1996, p. 21 et s. (« *Comparer, c'est toujours juger. C'est ainsi que le comparatiste qui choisit les problématiques et les questions directives de la recherche et qui procède à une définition du champ d'analyse, qui détermine quels sont les objets qui vont compter comme constituant du matériel à comparaison* » (*id.*, p. 51) ; « *le comparatiste doit sonder plus profondément l'arrière-plan social, culturel ou autre qui constitue tout discours juridique* » (*id.*, p. 33).

[188] Étienne PICARD, « L'état du droit comparé en France, en 1999 », art. préc., spéc. pp. 892-893. – V. ég. Gino GORLA, « Intérêts et problèmes de la comparaison entre le droit continental et la Common law », art. préc., spéc. p. 6.

[189] Rodolfo SACCO, *La comparaison juridique au service de la connaissance du droit, op. cit.*, spéc. n° 44, p. 106 (« *dans des pays divers, des lois identiques donnent lieu à des solutions pratiques différentes, que des solutions pratiques identiques sont le produit de lois différentes ou cohabitent avec des définitions savantes différentes ou sont mises en connexité avec des motifs opposés et incompatibles* »).

[190] Rodolfo SACCO, *La comparaison juridique au service de la connaissance du droit, op. cit.*, spéc. p. 8 (« *Si elle porte son attention sur ces multiples modèles, elle le fait pour établir en quelle mesure ils sont identiques et en quelle mesure ils sont différents* »). – V. ég. Yves-Marie LAITHIER, *Droit comparé*, Dalloz, coll. *Cours*, 2009, spéc. n° 1, pp. 1-2 et n° 8, p. 15 (« *Le comparatiste doit s'efforcer de comprendre l'étendue exacte des différences, leurs causes ainsi que leurs effets* »). – Étienne PICARD, « L'état du droit comparé en France, en 1999 », art. préc., spéc. p. 887 (« *Le droit comparé constitue* […] *cette discipline scientifique cherchant à connaître et surtout – à ce quoi, néanmoins, il ne tend pas toujours assez, en fait – à comprendre les droits étrangers* »).

73. Au-delà de cette fonction première, le droit comparé peut également permettre d'améliorer un droit interne [191]. Chaque droit est lié aux spécificités culturelles d'un pays, ses valeurs, ses traditions. Il en résulte inévitablement des différences entre les États, symptomatiques des priorités accordées par chacun d'eux. « *L'une des avancées les plus importantes de la pensée comparatiste contemporaine consiste précisément en l'attention donnée à cette perception critique de sa propre réalité juridique informée par un regard sur l'autre* » [192]. L'exercice de comparaison pourra dès lors permettre de découvrir des règles qui pourraient apparaître comme plus adaptées pour répondre aux besoins économiques ou sociaux face à un problème donné. Les systèmes juridiques étrangers peuvent donc être, à ce titre, une source d'inspiration riche dans la recherche constante d'une plus grande effectivité du droit. Toutefois, l'introduction éventuelle d'une notion ou d'une institution nouvelle imposera d'en vérifier l'opportunité [193]. Tel sera le cas lorsque nous envisagerons tout particulièrement l'éventuelle introduction, dans notre droit national, des dommages-intérêts punitifs ou encore de la *class action* existants aux États-Unis [194]. Il s'agira alors de déterminer si cette « *greffe d'une culture juridique sur une autre* » que Jean CARBONNIER désignait par l'expression d'« *acculturation juridique* » [195] est compatible avec le système juridique dans lequel elle a vocation à être implantée. À cet égard, cet illustre auteur mettait en garde contre toutes réussites qui seraient purement théoriques : « *si l'introduction des institutions étrangères se limitent à une modification des textes autochtones sans s'accompagner d'effectivité dans l'application, elle n'a pas de valeur sociologique* » [196]. Il ajoutait que la réussite de cette importation dépendait également de sa réception par la société. En effet, dans la mesure où « [u]*ne loi n'est pas seulement un texte avec les juges et*

[191] Jean CARBONNIER, *Droit civil, Introduction,* 27e éd., P.U.F., 2002, spéc. n° 26, p. 72 (« *Le droit comparé est, avant tout, un instrument de réforme législative. Le progrès du droit ne va point d'un pas égal dans tous les pays. Des lois étrangères peuvent ainsi fournir des modèles à imiter* »).

[192] Horatia MUIR WATT, « La fonction subversive du droit comparé », *RIDC* 2000, p. 503 et s., spéc. n° 18, p. 518.

[193] Mireille DELMAS-MARTY, « Du bon usage du droit comparé », *in* Mireille DELMAS-MARTY (sous la dir.), *Critique de l'intégration normative : L'apport du droit comparé à l'harmonisation des droits,* P.U.F., coll. *Les voies du droit,* 2004, p. 227 et s., spéc. pp. 228-231.

[194] V. *infra* : n° 478 et s. et 495 et s..

[195] Jean CARBONNIER, *Sociologie juridique,* 2e éd., Quadridge/P.U.F., 2004, spéc. p. 377 et s., spéc. p. 377 (« *Par acculturation juridique* […] *il faut entendre toute greffe d'une culture sur une autre* »).

[196] Jean CARBONNIER, *Sociologie juridique, op. cit.,* spéc. p. 377 et s. « *si tout est déterminé par le milieu social, il n'est pas de transplantation hors du milieu social qui ne soit pas une aventure et ne doive, à tout le moins, se solder par une déformation de l'élément transplanté. Peut être l'acculturation* (p. 380) *juridique se prêtera-t-elle à une appréciation plus nuancée, car tout dans le droit n'est pas déterminé, et l'on ne saurait éliminer la part que la volonté et la contrainte – la contrainte réussie – peuvent y prendre. Ce qui est exact, c'est que, dans l'acculturation, il faut se défier des réussites théoriques ; si l'introduction des institutions étrangères se limitent à une modification des textes autochtones sans s'accompagner d'effectivité dans l'application, elle n'a pas de valeur sociologique* » (*id.,* p. 381) *; Effets sur les individus :* « *Pour appliquer ce critère d'acculturation juridique il faut admettre que le droit ait fait partie dans la formation de la personnalité. De fait si le système juridique national contribue à modeler ce que l'on appelle la psychologie d'un peuple, il est plausible de supposer que l'implantation d'une institution étrangère se traduit* (*id.,* p. 382) *toujours par un certain changement dans les attitudes mentales des autochtones* (*id.,* p. 383) *».*

les praticiens qui l'appliqueront, c'est aussi le peuple auquel on prétend l'appliquer » [197], il convenait de s'assurer qu'une telle importation ne se heurte pas à un risque de rejet par cette dernière.

74. Justification du recours au droit américain. Nous avons fait le choix d'étudier l'approche américaine qui tend à construire un cadre juridique pour traiter du problème du *spamming* et qui est particulièrement importante pour une perspective européenne, et notamment française et ce, pour plusieurs raisons. Premièrement, la majorité des *spams* reçus par les internautes français provient des États-Unis et est destinée à un lectorat américain. Une étude récente révèle que, parmi les douze principaux pays émetteurs de *spams* entre les mois octobre à décembre 2010, les États-Unis conservent, sans surprise, la première place avec 18,83% du *spam* émis dans le monde (contre 15,2% au second trimestre 2010) [198]. Les États-Unis poursuivent donc leur progression et sont désormais responsables d'un message indésirable sur cinq, presque 2,5 fois plus que l'Inde qui leur succède immédiatement [199]. De tels courriers électroniques n'ont dès lors aucune pertinence pour les consommateurs français et peuvent ainsi être facilement classifiés comme du courrier électronique non sollicité. Bien que les utilisateurs de courriers électroniques français restent des acteurs passifs à cet égard, ils se trouvent néanmoins comme destinataires de quantités onéreuses de courriers indésirables américains et, ont par conséquent, un intérêt tout particulier à connaître quel régime juridique est adopté aux États-Unis pour lutter contre cette pratique. Deuxièmement, dans la mesure où les États-Unis ont été le premier pays à rencontrer un problème majeur avec le *spamming*, ils ont également été les précurseurs pour tenter de traiter le problème sur un fondement légal. Des leçons peuvent ainsi être tirées de l'expérience américaine, de l'approche adoptée et des erreurs faites. Enfin, la question de la protection des « spammés » prend un relief particulier dans la mesure où les législateurs français et américain adoptent des approches différentes en matière de protection des données à caractère personnel mais aussi en matière de réglementation du *spamming*. Ces divergences sont source de difficultés et de blocage lorsque le contentieux s'inscrit dans un cadre international.

---

[197] Jean CARBONNIER, *Droit civil, Introduction, op. cit.*, spéc. n° 31, p. 79 (« *Avant d'imiter une loi étrangère, le législateur français devrait s'assurer qu'elle trouvera en France le climat dont elle est environnée dans son pays d'origine* »).

[198] Selon une récente étude de SOPHOS, un éditeur de solutions anti-virus, les douze principaux pays relayant du spam pour la période d'octobre à décembre 2010 est la suivante : 1. États-Unis : 18,83% ; 2. Inde : 6,88% ; 3. Brésil : 0,4% ; 4. Russie : 4,64 ; 5. Royaume Uni : 4,54% ; 6. France : 3,45% ; 7. Italie : 3,17% ; 8. Corée du Sud : 3,01% ; 9. Allemagne : 2,99% ; 10. Vietnam : 2,79% ; 11. Roumanie : 2,25% ; 12. Espagne : 2,24%, Autres pays : 40,17% (" The top twelve spam relaying countries for october – December 2010 ", 11 janv. 2011, disponible sur : http://www.sophos.com/en-us/press-office/press-releases/2011/01/dirty-dozen-q42010.aspx).

[199] SOPHOS, « Classement trimestriel des douze pays relayeurs de *spam* », 14 oct. 2010, disponible sur : http://www.sophos.fr/pressoffice/news/articles/2010/10/dirty-dozen-q32010.html.

75. Les premiers jalons de notre recherche ainsi posés, il convient à présent de mettre en exergue **Les imperfections de la protection spéciale (Partie 1.)** qui imposeront **Un dépassement nécessaire de la protection spéciale (Partie 2.)**.

PREMIÈRE PARTIE

LES IMPERFECTIONS DE LA PROTECTION SPÉCIALE

76. Les menaces pesant sur les données à caractère personnel, matière première du *spamming*. Le *spamming* n'est rendu possible qu'à partir du moment où le « spammeur » est parvenu à collecter ou à générer l'adresse électronique des futurs destinataires de ces messages [200]. La numérisation des données a facilité leur accessibilité et leur captation : toute donnée diffusée en ligne est désormais susceptible d'être captée et exploitée par toute personne connectée au réseau, quelle que soit sa localisation géographique. Pour assurer le succès de leurs opérations, les « spammeurs » se livrent à une véritable traque des données à caractère personnel et notamment, des adresses électroniques diffusées sur le réseau, rendant ainsi les données de plus en plus vulnérables. Ces risques sont d'autant plus importants que dans la plupart des cas, la collecte et les traitements sont réalisés à l'insu de leurs titulaires.

77. L'évolution inquiétante du *spamming*. Une fois collectées, ces données nominatives seront utilisées par les « spammeurs » afin de procéder aux envois proprement dits. L'expédition de ce type de messages engendre alors des conséquences diverses : contre leur volonté, les titulaires de ces données verront leur boîte aux lettres électroniques inondée d'*e-mails* indésirables pouvant aller jusqu'à leur saturation en cas d'envois massifs. De même, l'afflux massif de *spams* est susceptible de paralyser partiellement voire totalement le réseau des FAI et les services de messageries des entreprises [201]. Par ailleurs, nous verrons que le *spamming* tend à évoluer, en délaissant progressivement sa finalité commerciale originelle, pour s'associer à d'autres techniques illicites, rendant ainsi les attaques de *spamming* de plus en plus agressives et dangereuses.

78. La recherche d'une protection efficiente. Dans ce contexte de menaces, une réflexion relative aux réponses juridiques destinées à assurer la protection des « spammés » et de leurs données nominatives s'impose naturellement, à la fois en amont, pour éviter que les adresses électroniques ne soient abusivement collectées, et en aval, afin de les prémunir contre des envois illicites. Toutefois, la recherche de réponses juridiques efficaces et adaptées aux réalités pratiques impose de prendre en compte le contexte dans lequel s'insère le *spamming*. Nous verrons que la protection des « spammés » relève d'un exercice particulièrement délicat. En effet, situé au croisement de diverses problématiques, le *spamming* mêle à la fois des contraintes d'ordre technique et des préoccupations économiques et sociales difficilement conciliables qui opposent les « spammeurs » aux

[200] V. *supra* : n° 58 et s.
[201] Sur les dommages causés par le *spamming*, v. *supra :* n° 46 et s.

« spammés ». Ce contexte conflictuel transparaît d'ailleurs à travers les divergences qui se manifestent entre les législations spéciales en vigueur, chaque législateur national adoptant une approche particulière de la protection des données à caractère personnel et consacrant une conception singulière du *spamming*. En effet, tandis que certains, plus enclins à protéger le commerce électronique, accordent une certaine indulgence à l'égard des « spammeurs », d'autres attachent une importance majeure à la priorité à la protection des données à caractère personnel et aux titulaires de ces données, « spammés » potentiels. Par ailleurs, la dimension intrinsèquement internationale du *spamming* ne permet pas d'ignorer ces profondes divergences qui se répercuteront inévitablement sur le comportement des « spammeurs » qui seront plus enclins à s'établir dans les pays où la législation apparaît la plus clémente envers cette pratique. Cette disparité entre les lois nationales conduira naturellement à s'interroger sur leur réelle capacité à protéger efficacement les « spammés ». Pour cela, il convient dans un premier temps d'identifier les différents défis factuels que pose le *spamming* et auxquels devront se confronter les législateurs (Titre I.). Nous examinerons dans un second temps les réponses légales actuelles face à ces différents défis et constaterons la fragilité des réponses légales (Titre II.).

TITRE PREMIER : LA MULTIPLICITÉ DES DÉFIS FACTUELS

79. La recherche d'une protection efficace des « spammés » implique tout d'abord d'identifier les causes justifiant ce besoin de protection. À cette occasion, nous verrons que le *spamming* constitue une réelle menace pour les données à caractère personnel, en particulier pour les adresses électroniques, qui subissent une véritable « traque » de la part des « spammeurs ». En effet, raison d'être du *spamming*, ces données à caractère personnel deviennent ainsi un enjeu crucial motivant les « spammeurs » à mener des opérations de collectes massives et le plus souvent, à l'insu de leurs titulaires. Face à des attaques de plus en plus agressives et expertes des « spammeurs » qui se manifesteront au stade de la collecte mais également lors de l'envoi des *spams,* les législateurs seront confrontés à un véritable défi pour tenter de mettre en place un régime suffisamment protecteur des données et de leurs titulaires. Par ailleurs, les législateurs devront prendre en compte le contexte économique et social dans lequel s'insère la problématique du *spamming.* Nous verrons que cette pratique suscite des sentiments contradictoires qui engendrent de profondes tensions entre les « spammés » qui revendiquent une protection forte de leur données et aspirent à la liberté de choisir de recevoir ou non des *e-mails* et les « spammeurs » et les « spammeurs » qui ont bien compris les enjeux économiques qui s'attachent aux données nominatives n'ont pas l'intention de céder à la pression.

80. Ainsi, nous verrons que la mise en place d'un système de protection efficace des « spammés » constituera une tâche particulièrement délicate pour les législateurs confronté à un double défi, non seulement technologique (Chapitre 1.) mais aussi socio-économique (Chapitre 2.).

CHAPITRE PREMIER : LE DÉFI TECHNOLOGIQUE

81. Le *spamming* expose les données nominatives à de perpétuelles menaces de collecte et de traitement à l'insu de leur titulaire. Dans une démarche sécuritaire, appréhender la réalité des risques encourus par ces données apparaît indispensable pour mieux les maîtriser et y faire face. Pour cela, notre propos est de comprendre en quoi le *spamming* constitue une menace pour les données à caractère personnel mais aussi pour le bon fonctionnement de la communication électronique et notamment l'usage des services de messagerie électronique. L'environnement technologique particulièrement hostile qui sera décrit (Section I.) permettra de dresser le bilan de l'état d'insécurité actuelle et de réfléchir aux moyens les plus adaptés pour lutter contre cette pratique. Face à la technicité du *spamming*, un réflexe naturel inciterait à se tourner vers des mesures de protection techniques. Toutefois, notre étude conduira à constater l'échec d'une réponse exclusivement technique (Section II.) [202].

[202] Pour une définition des termes techniques utilisés dans ces développements, nous renvoyons le lecteur au glossaire annexé à la fin de la thèse.

SECTION I. UN ENVIRONNEMENT TECHNOLOGIQUE HOSTILE

82. L'objectif de cette étude est de mettre en évidence que l'environnement numérique comporte des risques auxquels les internautes doivent être sensibilisés : toute navigation négligente et imprudente sur l'internet expose leurs données nominatives à des captations et utilisations abusives de la part des « spammeurs » (§ 1.), comme en témoigne leur *modus operandi* (§ 2.).

§ 1. DES DONNEES FORTEMENT EXPOSEES A DES CAPTATIONS ET UTILISATIONS ABUSIVES

83. Les espaces publics de l'internet, véritable eldorado pour les « spammeurs ». Certaines sociétés peu scrupuleuses ayant collecté de façon légale ou non des adresses électroniques, peuvent revendre leurs listes d'abonnés à des tiers à l'insu des personnes concernées. Les « spammeurs » profiteront de ces initiatives malveillantes pour acquérir de telles listes qui regorgent de données nominatives et qui viendront alimenter encore davantage les bases de données destinées à l'envoi de *spams.* Mais le plus souvent, les adresses électroniques sont collectées massivement dans les espaces publics de l'internet. En effet, à l'occasion de leur navigation sur l'internet, les internautes sont amenés à réaliser diverses opérations – participation à un forum de discussion (*newsgroup*), inscription à une liste de diffusion, abonnement à une lettre d'information (*newsletter*), etc. – qui nécessitent la communication d'une adresse électronique. Une fois divulguée, cette dernière pourra être facilement captée par le « spammeur » qui n'aura plus qu'à procéder, par la suite, à l'envoi de messages à cette adresse. Pour saisir cette réalité, reprenons plus en détails chacune des hypothèses illustrant les divers contextes dans lesquels ces collectes sont possibles.

84. Les forums de discussion. La collecte d'adresses électroniques est largement facilitée sur les forums de discussion dans la mesure où, le plus souvent, les participants rédacteurs les font apparaître dans leurs messages. Le « spammeur » en profitera alors pour les capter et envoyer des *spams* à ces contributeurs peu vigilants [203]. Par ailleurs, les serveurs de messagerie tels que *Microsoft Outlook*, *Mozilla Thunderbird*, etc., permettent de consulter hors ligne les archives des groupes, c'est-à-dire de conserver sur le disque dur de l'ordinateur de l'internaute toutes les conversations qui l'intéressent et de les consulter ultérieurement sans être connecté à l'internet. Le danger pourrait apparaître lorsqu'un virus s'est introduit

[203] Ces menaces ne sont pas nouvelles puisque dix ans auparavant, la CNIL alertait déjà des dangers de captation des adresses électroniques figurant dans les espaces de discussion à des fins commerciales (*Rapport d'activité 1998*, n° 19, Doc. fr., 1999, spéc. p. 95).

dans le poste de cet utilisateur dans la mesure où ce logiciel malveillant pourrait alors aspirer toutes les adresses présentes sur le disque dur.

85. L'inscription du « spammeur » à des listes de diffusion. La liste de diffusion est utilisée par un groupe partageant des intérêts communs qui discute et échange ensemble par courrier électronique sur un sujet particulier. Tout message expédié à l'adresse de cette liste est transmis par *e-mail* à l'adresse de chaque membre. L'inscription du « spammeur » lui permettra ainsi de profiter de la réception des messages rédigés par les autres membres et collecter ainsi les adresses électroniques des participants qui sont contenues dans ces messages. Une fois les adresses collectées, il suffira d'un simple envoi à une liste de diffusion pour que le même *spam* parvienne à tous ses membres [204]. En outre, cette technique est particulièrement efficace puisqu'elle permettra au « spammeur » de s'assurer du caractère actif de chacune des adresses d'expédition [205].

86. Les annuaires diffusés sur l'internet. Certains sites *Web* sont dédiés à la diffusion sur l'internet d'annuaires d'élèves, de membres, d'abonnés ou de personnels qui étaient le plus souvent déjà publiés sur d'autres supports (papier ou télématique). La diffusion en ligne de ces annuaires représente ainsi une occasion supplémentaire pour les « spammeurs » de collecter des adresses électroniques ou des numéros de téléphone très facilement.

87. Les chaînes de courriers électroniques (*hoax*). Les *hoaxes* sont des canulars ou des mauvaises blagues informatiques envoyés par courrier électronique, faisant croire aux destinataires qu'ils proviennent d'expéditeurs connus de ces derniers [206]. Le plus souvent, ces messages sont destinés à solliciter leur participation à une chaîne de solidarité, à les alerter de la présence de prétendus virus mais ils peuvent également véhiculer des informations fausses ou de nature à porter atteinte à la réputation et à l'image d'une société ou d'une personne physique [207]. Abusant de la crédulité des destinataires, ces derniers répandent spontanément les rumeurs en relayant cet *e-mail* de carnet d'adresses en carnet d'adresses, tout en conservant dans le champ des destinataires l'adresse de l'expéditeur initial, à savoir

[204] Sur les différentes techniques d'envoi de *spams*, v. *infra* : n° 95 et s.
[205] Sur la question de la vérification des adresses actives, v. *infra* : n° 94 et s.
[206] Pour une vision d'ensemble sur ces canulars, v. le site de Hoaxbuster, dédié à la lutte contre les *Hoax* et disponible à l'adresse suivante : http://www.hoaxbuster.com/.
[207] V. par exemple le *hoax* annonçant faussement la possibilté de gagner une caisse de champagne de la marque Veuve-Cliquot (consulter la page du site *Web* de hoaxbuster qui alerte des canulars circulant sur l'internet, mise à jour en 2003, disponible sur : http://www.hoaxbuster.com/hoaxliste/hoax.php?idArticle=864, dernière mise à jour 8 févr. 2003) ou encore le *hoax* qui en 2000, désignait le groupe pétrolier TOTAL FINA ELF comme responsable de la marée noire de l'Erika et encourageait le *boycot* de TOTAL (disponible sur : http://www.hoaxbuster.com/hoaxliste/hoax_message.php?idArticle=1609).

celle du « spammeur » [208]. Chaque nouveau transfert offre ainsi au « spammeur » l'opportunité d'intensifier sa collecte.

88. Les réseaux sociaux. Les sites de réseaux sociaux comme *Facebook, Twitter, MySpace, Linkedln* ou encore *Ping,* un réseau social musical nouvellement apparu, sont des espaces d'échanges désormais pleinement intégrés dans le quotidien de la plupart des internautes. Leur succès a également attiré les « spammeurs » et sont devenus des proies de plus en plus populaires auprès de ces derniers en raison de la quantité de données nominatives dont ils regorgent et qui sont constamment complétées et mises à jour.

89. Quelques règles élémentaires de prudence à observer. Au regard de l'ensemble de ces cas de figure, il convient d'admettre que les données à caractère personnel sont fortement exposées à des risques de collectes totalement opaques si leurs titulaires n'adoptent pas une attitude circonspecte lorsqu'ils sont amenés à les communiquer en ligne. En effet, tout acte qui semble en apparence anodin, peut devenir un véritable piège pour tout internaute imprudent [209]. Ainsi, la première protection de ces derniers reste la vigilance afin d'éviter la collecte et l'exploitation abusives de leurs données nominatives. Il est essentiel de laisser le moins de traces possibles des navigations opérées sur l'internet par le recours notamment aux *remailers* qui permettent de masquer l'adresse IP réelle du *proxy* de l'utilisateur en lui substituant un pseudonyme, de sorte que les sites visités ne détecteront que l'adresse IP du proxy utilisée [210]. Il est également impératif que tout utilisateur des services de l'internet réfléchisse avant de dévoiler sa véritable identité et évite de divulguer son adresse sans raison ainsi que celles d'autres personnes sans leur consentement [211]. Par ailleurs, en cas de réception d'un message dont l'origine se révèle douteuse, il convient de ne

[208] Afin que le « spammeur » puisse récupérer les adresses, il est nécessaire que le message précise qu'il faille conserver, outre les adresses des destinataires issues du carnet d'adresses de l'expéditeur du message, une adresse dans le champ « Cci », qui correspondra à celle du « spammeur » à l'origine de la chaîne d'envois. Étant ainsi en copie des messages envoyés, ce dernier pourra alors récupérer l'adresse électronique de chaque internaute participant à ladite chaine.

[209] Comme le souligne Jean FRAYSSINET, « [s]*ur l'Internet la traçabilité peut prendre des formes plus inquiétantes pour la protection des droits et libertés des personnes. On songe en particulier aux modes de collecte de données-traces à l'insu de la personne, sans information ni consentement préalables. Lors de la consultation d'un site, cliquer sur un bandeau publicitaire ou sur des liens hypertextes n'est pas un acte neutre* » (« La traçabilité des personnes sur l'internet, une possible menace pour les droits et libertés », *in* Philippe PEDROT (sous la dir.), *Traçabilité et responsabilité*, Economica, 2003, p. 88 et s., spéc. n° 13, p. 97.

[210] Il est aussi possible d'utiliser une boîte aux lettres gratuite chez un fournisseur de messagerie qui agit comme un anomyseur et en lui proposant de choisir un pseudonyme pour constituer une nouvelle adresse électronique et ainsi dissimuler sa véritable identité.

[211] Par exemple, à l'occasion de la création d'un groupe de discussion, d'une liste de diffusion, il est important lors du transfert d'un message aux participants de ce groupe ou aux membres de cette liste, de conserver l'anonymat des destinataires. Afin d'éviter que des robots ne récupèrent des adresses électroniques figurant dans les espaces publics de l'internet, il convient notamment d'utiliser la fonction « copie cachée » (CCI) du logiciel de messagerie, de limiter la participation à des chaînes d'*e-mails* ... Si l'internaute souhaite tout de même participer à ces chaînes, il doit s'assurer que les adresses électroniques des destinataires sont en « copie cachée ». À défaut, le « spammeur » pourra s'en servir pour collecter des adresses valides.

pas l'ouvrir et encore moins d'y répondre. En effet, s'il s'avère que le message est un *spam*, le fait de le consulter ou d'y répondre indiquera au « spammeur » que l'adresse est valide et consultée et l'incitera alors à poursuivre ses envois vers ce destinataire [212]. Enfin, à la réception d'un SMS ou d'un MMS frauduleux, il est important que les victimes contactent la plate-forme de gestion des alertes de messages frauduleux, mise en place en octobre 2008 et désormais étendu aux *spams* vocaux depuis juin 2010, en composant le « 33700 » [213]. Lorsqu'un numéro est signalé à plusieurs reprises comme douteux, cette plate-forme rappelle ce numéro afin de prendre connaissance du message enregistré. Afin de vérifier que l'alerte est exacte, la plate-forme vérifie que le contenu du message est conforme à l'activité déclarée dans le contrat par l'éditeur, l'entreprise qui propose le service (voyance, achat de sonneries téléphoniques, …). En cas de non respect du contrat, l'opérateur procède à la suspension de la ligne pour stopper immédiatement la fraude. Chaque année des centaines de lignes subissent le même sort. Certes, cette solution a ses limites puisque le « spammeur » peut toujours ouvrir une nouvelle ligne afin de proposer un nouveau service frauduleux, toutefois, la mise en place de ce dispositif d'alerte participe activement à la lutte contre le *spamming* par téléphone (*ping call*) [214]. Selon le communiqué de presse rendu par Hervé NOVELLI, secrétaire d'État chargé du commerce, 787.000 SMS ont été signalés depuis la mise en place de ce dispositif en octobre 2008. Parmi ce volume, 555.000 comportaient des renvois vers des numéros surtaxés. Ces signalements ont permis aux opérateurs de communications électroniques d'adresser aux éditeurs indélicats plusieurs dizaines de mises en demeure chaque mois. Dans 790 cas, les opérateurs de mobile avaient coupé l'accès au numéro de téléphone identifié [215]. En état de cause, il convient néanmoins de souligner qu'une attitude de prudence des internautes suppose qu'en amont, ils soient mieux informés et sensibilisés quant aux risques de collecte « sauvage » de leurs données à caractère personnel [216].

---

[212] Une étude menée en 2009 et réalisée auprès de 800 personnes aux États-Unis et au Canada par le *Messaging Anti-Abuse Working Group* rapporte que plus d'un tiers des consommateurs reconnaissent répondre à des *e-mails* qu'ils soupçonnent pourtant être des *spams*, la moitié des consommateurs qui utilise un logiciel antivirus, dit ne jamais cliquer sur un message qu'il soupçonne être du *spam* et 21% des personnes interrogées ne prend aucune disposition particulière pour empêcher que des *spams* atteignent leur boîte de réception (" Hey, Why Did You Reply to that Spam?", 2009, disponible sur : http://www.maawg.org/node/431).

[213] V. le site de sensibilisation, disponible sur : http://www.33700-spam-sms.fr/

[214] Ce dispositif est également renforcé par l'action de l'office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC) créé en 2000 , compétent en matière d'intrusions dans les systèmes de traitements automatisés de données, de fraudes aux communications téléphoniques, d'infractions à la loi informatique, fichiers et libertés, d'utilisations frauduleuses de numéros de carte bancaire … (sur cet office, consultez les adresses suivantes :
http://www.securiteinfo.com/legal/OCLCTIC.shtml;
http://www.interieur.gouv.fr/sections/a_l_interieur/la_police_nationale/organisation/dcpj/cyber-criminalite).

[215] Hervé NOVELLI, « Lutter contre les *spams* par SMS et vocaux et les prospections téléphoniques non désirées », Communiqué de presse, 21 juin 2010, disponible sur :
http://www.economie.gouv.fr/presse/dossiers_de_presse/100621spam.pdf.

[216] Yves POULLET, « Mieux sensibiliser les personnes concernées, les rendre acteurs de leur propre protection », *RLDI* mai 2005, n° 152, p. 47 et s. – V. ég. le Comité des ministres aux États membres sur la protection de la vie

§ 2. LES REALITES PRATIQUES DE LA MENACE : LE *MODUS OPERANDI* DES « SPAMMEURS »

90. Délimitation de l'étude. L'analyse du processus d'envoi de *spams* n'a pas pour finalité de recenser l'ensemble des techniques utilisées par les « spammeurs ». Une telle démarche se révèlerait particulièrement laborieuse dans la mesure où les aspects techniques sont totalement abscons pour la plupart des profanes. Même à supposer que ces techniques soient comprises, leur rapidité d'évolution associée à l'imagination toujours plus créative des « spammeurs » pour déjouer les mesures anti-*spam*, les rend très rapidement obsolètes. Notre objectif est donc plutôt de comprendre, à travers le *modus operandi* des « spammeurs », quels sont les risques encourus par les données à caractère personnel et par ricochet, les répercussions sur la communication électronique, qui justifient une protection forte des « spammés » à la hauteur des menaces identifiées. Pour cela, il conviendra de décrire de façon chronologique les diverses étapes qui aboutiront à l'envoi de *spams*. Nous débuterons cette étude par la description des techniques de collecte des adresses électroniques, opération préalable à toute activité de *spamming* (A.) avant d'exposer les divers procédés de vérification auxquels ont recours les « spammeurs » pour s'assurer du succès de leur opération (B.). Une fois la collecte et les vérifications effectuées, ils n'auront plus qu'à procéder aux envois proprement dits, expression concrète du *spamming.* À ce stade ultime, nous verrons que les techniques d'envois sont devenues de plus en plus pernicieuses et efficaces et contribuent à accroître le caractère agressif de cette pratique (C.). Cette dangerosité du *spamming* se manifestera également à travers ses différentes mutations (D.).

A. LES TECHNIQUES DE COLLECTE DES ADRESSES ELECTRONIQUES

91. Outre les hypothèses de collecte *via* l'inscription à un forum de discussion ou à une liste de diffusion, le « spammeur » opérera le plus souvent en recourant à des procédés qui lui permettront d'opérer à grande échelle et de mener, en particulier, des collectes intensives et encore plus efficaces.

privée sur Internet recommandait déjà en 1999 aux FAI d'« [i]*nforme*[r] *les utilisateurs des risques que l'utilisation d'Internet fait courir à la vie privée, avant qu'ils ne souscrivent ou commencent à utiliser des services. Il peut s'agir de risques concernant l'intégrité des données, leur confidentialité, la sécurité du réseau ou d'autres risques liés à la vie privée, tels que la collecte ou l'enregistrement de données effectués à leur insu* » (Recommandation n° R (99) 5, « *Lignes Protectrices pour la protection des personnes à l'égard de la collecte et du traitement de données à caractère personnel sur les "inforoutes"* », 23 févr. 1999, spéc. p. 4, disponible sur : https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=276586&SecMode=1&DocId=396770&Usage=2).

92. Des logiciels spécialement conçus pour faciliter la collecte. Il existe des robots malveillants, les *spambots*, programmés pour parcourir sans cesse le réseau à la recherche du signe « @ », indicateur de la présence d'adresses électroniques (*mail harvesting*). Une fois les adresses détectées, celles-ci seront aspirées par ces logiciels qui scanneront ensuite les autres sites liés aux précédents en procédant de la même façon [217]. Grâce à ce type de robot d'indexation (*web crawler* ou *web spider*), le « spammeur » pourra ainsi, de liens en liens, engranger une quantité très importante d'adresses électroniques lui permettant de constituer de vastes listes de diffusion (*mailing list*) en un laps de temps très court et à moindre coût [218].

93. L'attaque dite « dictionnaire » : la génération aléatoire d'adresses. Le « spammeur » pourra recourir au piratage d'annuaires, encore appelé attaque DHA (*Directory Harvest Attack*). Cette technique consiste à reconstituer des adresses électroniques à partir d'une combinaison classique, la plupart des internautes disposant d'au moins une adresse associant ses nom et prénom. À l'aide d'un logiciel capable de générer de façon aléatoire des centaines de milliers d'adresses électroniques [219], le « spammeur » élabore un premier dictionnaire à partir des noms patronymiques les plus usuels d'un pays (par exemple, Dupont Durand, Martin, Marchand…). Un second dictionnaire est composé des prénoms les plus courants de ce même pays (Pierre, Paul, Nicolas, Marie, etc. ...) et enfin un troisième regroupe les domaines de ce pays et les plus connus au niveau international (free.fr, wanadoo.fr, neuf.fr, club-internet.fr, msn.fr, Yahoo France, laposte.fr, aol.fr, hotmail.com, gmail.com…) [220]. À partir de ces listes, le logiciel testera toutes les combinaisons d'adresses possibles pour tenter de retrouver des adresses électroniques valides [221].

---

[217] Pour déjouer ces logiciels aspirateurs, l'idée pourrait être de remplacer l'arobase (@) de l'adresse électronique par « at » dans la mesure où la plupart des « extracteurs » d'*e-mails* ne sont pas en mesure de les repérer.

[218] Pour une démonstration de cette technique, consulter le site de CASPAM, disponible sur : http://www.caspam.org/emails-spam.html.

[219] Ces logiciels, spécifiquement programmés pour collecter, valider les adresses électroniques et leur envoyer des *e-mails*, sont facilement accessibles sur l'internet, de nombreux sites internet en proposant la vente. Tel est le cas par exemple du logiciel « *Prospect Mailer* », disponible sur : http://www.marketing-2000.net/pm.html, « *Email Collector Power 3,3* », disponible sur : http://power-email-collector.software.informer.com/3.3/. – Pour de nombreux autres exemples de ce type de logiciel téléchargeable en ligne, consulter la page *Web* disponible sur : http://software.informer.com/getfree-super-sonic-email-collector-2009/.

[220] Par exemple, à partir du nom patronymique « Marchand » et du domaine « laposte.fr », de multiples combinaisons sont possibles en utilisant les prénoms français les plus courants : marchand.pierre@laposte.fr, marchand.paul@laposte.fr, marchand.nicolas@laposte.fr, pierre.marchand@laposte.fr, paul.marchand@laposte.fr, nicolas.dupont@laposte.fr, pierremarchand@laposte.fr, paulmarchand@laposte.fr, nicolasmarchand@laposte.fr, etc.

[221] Schématiquement, le test consiste à envoyer à un DNS du domaine une demande d'autorisation pour envoyer un message à une adresse donnée. Toutes les combinaisons pour lesquelles le DNS répond par l'affirmative confirmera l'existence et la validité de ces adresses.

B. LES TECHNIQUES DE VERIFICATION DE LA VALIDITE DES ADRESSES

94. Une prudence accrue : des envois de plus en plus sûrs. Une fois que les bases de données regroupant les adresses collectées sont créées, le « spammeur » doit vérifier que chaque adresse d'expédition est active afin de s'assurer de la bonne réception du message par le destinataire. À cette fin, il aura recours à une combinaison de plusieurs techniques. Selon les résultats des recherches menées par la société BITDEFENDER, une société créatrice de solutions de sécurité [222], la première méthode consiste à exploiter les accusés de réception ou les avis de lecture d'un message, caractéristique commune à la plupart des logiciels de messagerie. Si par méfiance, l'utilisateur décide de ne pas envoyer l'accusé de réception, le « spammeur » utilise un autre procédé qui consiste à insérer un lien sur une page ou un site *Web* vers une image stockée sur un serveur *Web* distant administré par l'émetteur du message. En plaçant dans cette page ou sur ce site *Web* un pixel invisible (« *Web bug* »), le « spammeur » peut ainsi surveiller à distance le téléchargement de cette image à l'insu de l'utilisateur et être prévenu lors de sa visualisation. Toutefois, les clients de messagerie bloquent généralement ce type de contenu, ce qui oblige les utilisateurs à accepter le chargement de l'image pour la visualiser. L'affichage de celle-ci se fait par l'appel d'un programme sur le site de l'émetteur, en précisant un nombre identifiant l'adresse électronique du destinataire. Le programme valide l'adresse électronique associée au numéro et renvoie le graphique sollicité. Lorsque le client de messagerie affiche le message, il télécharge automatiquement l'image indiquée et le serveur *Web* de l'expéditeur est alors alerté que le message est en cours de visualisation et donc que cette adresse électronique est valide. En cas d'échec de ces deux niveaux de confirmation, le « spammeur » peut encore piéger le destinataire par le biais d'un faux lien de désinscription. La plupart des listes de diffusion de *spams* contient un lien qui permet en apparence au destinataire de se désinscrire. Lorsque ce dernier clique sur ce lien, il reçoit un message lui confirmant cette supposée désinscription mais en réalité, ce clic confirmera la validité de son adresse électronique, c'est-à-dire que celle-ci est active, et l'exposera encore davantage à la réception de *spams*. Enfin, il est possible que le « spammeur » examine les rapports de non-remise (NDR) qui sont renvoyés à l'expéditeur du message en cas d'adresse d'expédition invalide. Toute adresse qui renvoie ce rapport est considérée comme non valide et est alors supprimée de la liste d'envois du « spammeur ». Il arrive toutefois que l'envoi des NDR soit désactivé, l'absence de leur retour ne garantit alors pas que l'adresse n'est plus valide. Pour surmonter cet aléa, le

[222] Selon la société BITDEFENDER, les « spammeurs » tentent de piéger les internautes en les poussant à confirmer la validité de leur adresse électronique (Communiqué de presse, 9 oct. 2008, disponible sur : http://www.editions-profil.eu/EP/RessourcesSiteProfil/Communiques/BitDefender%20et%20la%20technique%20des%20*spams*.pdf.

« spammeur » analyse les messages d'absence de bureau ou inclut une demande d'accusé de réception dans les messages.

C. DES TECHNIQUES D'ENVOIS DE PLUS EN PLUS PERNICIEUSES ET AGRESSIVES

95. La dissimulation de l'origine des messages. Lorsque les listes d'adresses électroniques valides sont constituées, le « spammeur » peut commencer à procéder à l'envoi de *spams*. Afin d'éviter qu'ils ne soient identifiés par les filtres anti-*spam*, certains « spammeurs » utilisent leur propre machine en masquant l'origine des messages expédiés, soit en falsifiant leur adresse électronique (*spoofing*), soit en recourant à des *remailers* anonymes. D'autres « spammeurs » envoient des *spams* depuis des serveurs de location localisés dans des pays où la législation est suffisamment souple pour que le propriétaire du serveur ne soit pas mis en cause trop rapidement quand un utilisateur l'exploite pour des activités illicites (Asie, Europe centrale ou encore dans les pays de l'ex-URSS). Enfin, l'envoi de *spams* peut également être réalisé à partir de serveurs de messagerie non sécurisés autorisant tout envoi sans authentification préalable de l'expéditeur (relais ouvert ou *open relay*) [223]. Toutefois, cette solution les contraint à rechercher ces relais ouverts, opération qui prend du temps et occasionne des dépenses financières importantes puisque les « spammeurs » devront utiliser des robots destinés à les repérer sur le réseau pour ensuite les infiltrer. Outre cet inconvénient, il convient de noter, de façon plus générale, que l'efficacité de l'ensemble de ces techniques d'envois est affaiblie puisque les *remailers*, comme les serveurs de location ou les relais ouverts, peuvent rapidement être détectés et répertoriés sur des listes noires [224]. Pour échapper à ces difficultés, les « spammeurs » utilisent des méthodes de plus en plus sophistiquées pour poursuivre leur activité comme en témoigne, par exemple, la première exploitation du protocole IPv6 par les « spammeurs » en janvier 2010 pour envoyer des *spams* [225].

96. Le *mail bombing*. Les « spammeurs » peuvent également avoir recours à une forme d'envoi particulièrement agressive : le *mail bombing*. Ce type d'attaque consiste à envoyer une quantité considérable d'*e-mails* vers un destinataire unique dans le seul dessein de saturer la boîte aux lettres électroniques ou le réseau de la victime ou encore de paralyser sa bande passante.

---

[223] Ces diverses techniques – *spoofing* et *open relay* – ne sont ici que mentionnées dans la mesure où un développement leur sera consacré dans une autre partie de ce chapitre (v. *infra* : n° 137 et s).
[224] Sur le fonctionnement des listes noires, v. *infra* : n° 114 et s.
[225] SOPHOS, *Rapport sur les menaces à la sécurité*, 2010, spéc. p. 17, disponible sur : http://www.sophos.fr/sophos/docs/fra/papers/sophos-security-threat-report-jan-2010-wpfr.pdf.

97. La transformation des PC en « zombies » : la technique d'envois la plus redoutable. Si à ses débuts le *spamming* pouvait être considéré comme une simple source de nuisance, cette pratique s'est progressivement transformée en instrument de fraude. Cette évolution transparaît clairement à travers une connivence de plus en plus fréquente entre les pirates informatiques et les « spammeurs », les premiers exploitant les pratiques des seconds pour propager leurs virus tandis que les seconds profitent des techniques mises au point par les premiers pour multiplier les envois de *spams* [226]. Cette méthode « virale » est la plus agressive et la plus dangereuse car elle permet aux « spammeurs », par le biais de virus installé sur un ordinateur, d'en prendre le contrôle à l'insu de son propriétaire pour envoyer des *spams*. Ces PC zombies (*bots*) sont généralement créés à la suite de la découverte de failles dans les systèmes informatiques qui sont alors exploitées pour introduire des logiciels malveillants (*malware*) dans ces systèmes. Techniquement, lorsque les virus ont infecté un nombre suffisant d'ordinateurs – ces ordinateurs compromis formant ainsi un réseau de zombies (*botnet*) –, le « spammeur », administrateur de ces zombies, active alors ces virus restés en sommeil [227]. Chaque ordinateur contrôlé à distance, qui reçoit des instructions relatives au contenu des *e-mails* à envoyer, accompagnées d'une liste d'adresses différentes pour chacun d'eux, opère ensuite le transfert massif des *e-mails* comme un simple serveur d'*e-mails* (protocole de communication SMTP). À la fin du processus d'envoi des s*pams*, les *malwares* se remettent en veille jusqu'à leur nouvelle activation par le « spammeur ». Cette technique, particulièrement efficace, est de plus en plus répandue à tel point qu'elle représente désormais 80% des *spams* envoyés [228]. Son succès s'explique essentiellement pour trois raisons. D'une part, elle permet au « spammeur » d'agir anonymement et de contourner ainsi le blocage des messages qui seraient expédiés depuis des adresses déjà répertoriées sur des listes noires ou signalées automatiquement comme étant du *spam* par les serveurs de courrier électronique. D'autre part, son efficacité est incontestable puisqu'elle permet d'expédier des millions d'*e-mails* depuis des machines infectées dans un espace de temps très court [229]. Enfin, ce genre d'attaque est particulièrement lucratif puisque le gain s'élève en moyenne à un montant compris entre 50.000 et 100.000 dollars par an pour un

[226] Sur l'association entre *spams* et virus, v. *infra* : n° . 98 et s. – Dès 2005, la Commission fédérale du commerce américaine (FTC) avait relevé une évolution des techniques employées par les « spammeurs » et la progression des *botnets*, (v. FTC, *Effectiveness and enforcement of CAN-SPAM Act – A Report of Congress*, déc. 2005, spéc. p. 16, disponible sur : http://www.ftc.gov/reports/canspam05/051220canspamrpt.pdf).

[227] Sur la corrélation entre les *spams* et les réseaux de zombies, v. OCDE, *Les logiciels malveillants (maliciels) : Une menace à la sécurité de l'économie de l'Internet*, rapport préc., spéc. pp. 22-28.

[228] Selon les chiffres communiqués par KAPERLY LAB, une entreprise de sécurité informatique internationale, v. Yuri NAMESTNIKOV, " The economics of botnet ", 2009, disponible sur : http://www.securelist.com/en/downloads/pdf/ynam_botnets_0907_en.pdf.

[229] Le *botnet* Rustock, principal émetteur de *spams*, a été à l'origine de 41% des *spams* envoyés en 2010 : les PC zombies qui le composent peuvent envoyer 46 milliards de *spams* chaque jour, c'est-à-dire 32 millions par minute ou 192 *spams* par minute et par *bot* (Daren LEWIS, " The recent drop in global spam volumes – what happened ? ", 6 oct. 2010, disponible sur : http://www.symantec.com/connect/blogs/recent-drop-global-spam-volumes-what-happened).

prix unitaire du *bot* variant entre 5 et 1.000 dollars selon le type d'opérations qu'il lui est demandé d'effectuer [230].

D. LES MUTATIONS DU *SPAMMING*

98. Les diverses mutations du *spamming* se manifestent à travers, non seulement les multiples médias électroniques ciblés par les « spammeurs » (1.), mais aussi les techniques auxquelles ils ont recours. Exploitant les opportunités offertes par les nouvelles technologies, le *spamming* se décline désormais sous la forme d'attaques de plus en plus agressives, relayant au second plan sa finalité commerciale pour devenir une pratique malveillante [231](2.).

1. Des cibles d'envoi multiples

99. Le *spam* sur les espaces de discussion : forums et *blogs*. Devançant les *spams* envoyés par courrier électronique, les premiers *spams* sont apparus sur le réseau *Usenet* [232], les forums de discussion constituant des cibles particulièrement stratégiques pour les « spammeurs », tant pour la collecte d'adresses électroniques, comme nous avons eu l'occasion de le constater précédemment [233], que pour l'envoi de *spams*. En ce qui concerne cette dernière opération, son impact est relativement large puisque la transmission d'un message à un forum permet d'inonder simultanément les messageries de tous les participants. Par ailleurs, à l'instar des forums de discussion, les *blogs* sont apparus comme de plus en plus parasités par des commentaires indésirables. À cet égard, SOPHOS, l'un des plus importants éditeurs de sécurité informatique et de protection des données, a précisé dans son rapport de 2010 relatif aux menaces contre la sécurité, que sur l'ensemble des commentaires publiés sur les *blogs*, 83 % d'entre eux sont du *spam* [234]. Le rapport explique que cette

[230] V. Vitaly KAMLUK, " Botnet business ", 13 mai 2008, disponible sur : http://www.viruslist.com/fr/analysis?pubid=200676152 (cet article explique très bien le fonctionnement des réseaux de zombies, leurs avantages pour les « spammeurs »).
[231] SOPHOS, " Dirty dozen : USA number one culprit as spam becomes more malicious ", 11 janv. 2011, disponible sur : http://www.sophos.com/en-us/press-office/press-releases/2011/01/dirty-dozen-q42010.aspx.
[232] Sur *Usenet*, est considéré comme du *spam* tout article, quel que soit son contenu, et publié en un nombre d'exemplaires excessif et ce même s'il n'appartient pas aux catégories courantes de messages abusifs (publicités commerciales, escroqueries...) : tous les exemplaires d'un tel article peuvent alors être annulés par les utilisateurs (v. le site d'*Usenet* disponible sur *:* http://www.usenet-fr.net/usenet.html). – V. ég. « Comment réagir face aux messages abusifs », disponible sur : http://www.usenet-fr.net/fur/usenet/abus/reagir-general.html.
[233] V. *supra* : n° 83 et s.
[234] SOPHOS, *Rapport sur les menaces à la sécurité*, 2010, rapport préc., spéc. p. 17. – Face à ce phénomène, l'OCDE notait déjà en 2006 que « *La montée du phénomène porte atteinte à la fonctionnalité des blogs et aggrave le problème de la fiabilité de l'information sur l'Internet* » (*Rapport du Groupe de réflexion sur le spam*

situation perdure notamment en raison de la politique menée par les sites qui autorisent le dépôt de commentaires sans aucune modération afin de mettre en place une communauté active de participants [235].

100. Le *spam* sur les messageries électroniques « classiques » et les messageries instantanées. Historiquement limités aux forums de discussion d'*Usenet*, les envois de *spams* ont rapidement envahi les messageries électroniques. Quantitativement, ce type de *spam* par courrier électronique est aujourd'hui le plus usuel, notamment parce qu'il présente l'avantage de répercuter les coûts découlant de leur émission, directement sur les destinataires [236]. Malgré les mesures techniques mises en place par les fournisseurs de messagerie et les efforts déployés pour éviter que les postes de leur client ne deviennent des zombies, le résultat a été largement décevant. Tel a été le cas en octobre 2009 où une fuite de données, qui comportait des identifiants de connexion, avait permis d'accéder à des dizaines de milliers de comptes *Hotmail*, *Gmail*, *Yahoo*! *Mail*, AOL [237]. Pour leur part, les messageries instantanées telles que *Windows Live Messenger*, *Yahoo ! Messenger*, *Skype*, *Google Talk* … sont devenues une cible importante de propagation de ce type de *spams*, encore connus sous l'acronyme « SPIM » (« *Spam Over Instant Messaging* »). Les « spammeurs » exploitent, par exemple, des comptes d'utilisateurs piratés comme plates-formes de diffusion de liens infectés ou d'attaques de *phishing* [238].

101. Le *spam* sur la téléphonie mobile et la téléphonie sur IP. Devenus « *le vecteur de nouvelles formes de commerce électronique* » [239], les téléphones portables comptent désormais, eux aussi, parmi les cibles des « spammeurs ». Ces derniers sont en effet exposés non seulement à la réception de *spams* sous la forme de SMS, mais aussi de *spams* vocaux. s'agissant de ce dernier type de *spam*, le processus peut être ainsi décrit : le « spammeur » contacte massivement par téléphone des correspondants et raccroche à la première sonnerie afin que l'appel ne lui soit pas facturé. L'auteur de telles manœuvres compte sur la crédulité de certaines des milliers de personnes contactées pour rappeler le

de l'OCDE : Boîte à outils anti-spam de politiques et mesures recommandées, DSTI/CP/ICCP/*SPAM*(2005)3/FINAL, 19 mai 2006, spéc. p. 24, disponible sur : http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/CP/ICCP/SPAM(2005)3/FINAL&docLanguage=Fr.

[235] SOPHOS, rapport 2010 préc., spéc. p. 17.

[236] Sur cette répercussion des coûts du *spams*, v. *supra* : n° 8

[237] SOPHOS, rapport 2010 préc., spéc. p. 15.

[238] SOPHOS, rapport 2010 préc., spéc. p. 17.

[239] Thibault VERBIEST et Étienne WERY, « Commerce électronique par téléphone mobile (m-commerce) : un cadre juridique mal défini », *D.* 2004, chron., n° 41, p. 2. – Sur l'essor du commerce mobile, v. OCDE, *Le commerce mobile*, DSTI/CP(2006)7/FINAL, 9 févr. 2007, disponible sur : http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/CP(2006)7/FINAL&docLanguage=Fr.

numéro surtaxé. L'efficacité de cette parade tient au fait que les victimes portent rarement plainte et même dans le cas où elles décideraient d'agir, cette démarche ne sera entreprise qu'une fois la réception de la facture au montant exorbitant, ce qui laisse suffisamment de temps au malfaiteur pour effacer toutes traces de sa supercherie [240]. Par ailleurs, il convient de signaler l'apparition des *Blue spams*, une nouvelle forme de *spam* qui tend actuellement à se développer. Il s'agit de messages électroniques envoyés, sur un téléphone portable, à travers le réseau *Bluetooth* lorsqu'une personne passe à proximité d'un panneau publicitaire placé dans un lieu public (métros, cafés, voie publique,…) et équipé d'un dispositif d'envoi *Bluetooth*. Quant au « SPIT » (« *Spam Over Ip Telephony* »), cette nouvelle forme de *spam* touchant la téléphonie sur IP, même si son essor reste encore timide, la baisse de ces coûts liés à l'envoi de communications vocales que permet le protocole Voix sur IP (VOIP), risque à terme d'accroître cette nouvelle forme de *spams*.

102. Les sites de réseaux sociaux, nouvelles cibles du *spamming*. Victimes d'un succès très rapide, ces réseaux sociaux n'ont pas encore pris les mesures de sécurité suffisantes pour protéger leurs utilisateurs comme l'ont fait, depuis quelques années, les services de messageries électroniques telles qu'*Hotmail, Gmail* ou encore *Yahoo.* Ainsi, dans son rapport pour 2010 précité, SOPHOS a signalé que le nombre d'entreprises victimes de *spams* et de programmes malveillants *via* les réseaux sociaux avaient augmenté de 70% au cours de l'année 2009 [241]. En effet, le nombre d'entreprises ayant fait l'objet d'attaques de *spamming via* les sites de réseaux sociaux a fortement augmenté, passant de 33,4% en avril 2009 à 57% en décembre 2009 [242]. Par ailleurs, les experts de SOPHOS ont découvert, qu'une semaine après le lancement du réseau social musical *Ping* en septembre 2010, ce dernier était déjà envahi de *spams* [243]. Ils ont enfin relevé une hausse du *spam* diffusé sur les réseaux sociaux au troisième trimestre 2010, avec notamment le très médiatisé programme « onMouseOver » qui générait des *spams* sous forme de courts messages (*tweets*) sur *Twitter* [244]. Le rapport de Sophos de 2011 révèle une forte augmentation du *spamming* sur les

[240] Toutefois, l'extension du dispositif d'alerte « 33700 » au *spam* vocal depuis juin 2010 pourrait participer activement à la lutte contre le *spam* mobile dans son ensemble (sur ce dispositif d'alerte, v. *supra :* 89).
[241] SOPHOS, rapport 2010 préc., spéc. p. 3.
[242] SOPHOS, rapport 2010 préc., spéc. p. 3. – V. ég. Benjamin FERRAN, « Une faille de *Twitter* utilisée pour propager du *spam* », 21 sept. 2010, disponible sur : http://www.lefigaro.fr/web/2010/09/21/01022-20100921ARTFIG00500-une-faille-de-twitter-utilisee-pour-propager-du-spam.php.
[243] SOPHOS, « À peine le nouveau service Ping de Apple lancé, les spammeurs l'inondent d'arnaques sur iPhone », 3 sept. 2010, disponible sur : http://www.sophos.fr/pressoffice/news/articles/2010/09/ping.html.
[244] SOPHOS, « Classement trimestriel des douze principaux pays relayeurs de *spams* : la France premier émetteur européen », 14 oct. 2010 disponible sur : http://www.sophos.fr/pressoffice/news/articles/2010/10/dirty-dozen-q32010.html.

réseaux sociaux : alors que cette menace représentait 33,4% en avril 2009, elle passe à 57% en décembre 2009 pour atteindre 67% en 2010 [245].

2. Du *spamming* commercial au *spamming* malveillant

103. Si le *spamming* avait initialement une vocation commerciale, cette pratique a progressivement permis d'accomplir des actes malveillants [246], comme en témoignent la connivence entre un « spammeur » et un auteur de virus (a.) et les hypothèses où le *spamming* devient le vecteur d'escroqueries (b.).

a. La connivence entre « spammeur » et auteur de virus

104. Une première hypothèse de collusion entre un auteur de virus et un « spammeur » peut naître de la création d'un logiciel malveillant qui permet à d'autres utilisateurs de contrôler à distance des postes informatiques à l'insu de leur utilisateur légitime. En exploitant les failles de sécurité sur des navigateurs *Web*, le virus tente d'infiltrer l'ordinateur ciblé depuis un site Internet visité par un utilisateur. Une fois que le virus est parvenu à l'infecter, son auteur est alerté par le biais d'un message d'alerte qui lui permettra d'établir ensuite la liste des ordinateurs compromis. Cette liste pourra être transmise à un « spammeur » avec qui il s'est associé et qui n'aura plus qu'à utiliser ces postes comme plateformes d'envoi de *spams* (PC zombie) [247]. De cette façon, les propriétaires des ordinateurs infectés deviennent, à leur insu, les expéditeurs officiels de *spams* [248], un stratagème efficace pour les « spammeurs » qui leur permettent d'agir de façon anonyme. Un autre cas de figure consiste à insérer un virus dans la ou les pièces attachées à l'*e-mail* envoyé [249] ou intégré au message lui-même, notamment par l'insertion de liens

[245] SOPHOS, *Security Threat Report*, 2011, disponible sur : http://www.sophos.com/en-us/press-office/press-releases/2011/01/threat-report-2011.aspx.
[246] V. SOPHOS, " Dirty Dozen : USA number one culprit as spam become more malicious", 11 janv. 2011, disponible sur : http://www.sophos.com/pressoffice/news/articles/2011/01/dirty-dozen-q42010.html.
[247] Sur ce sujet, v. par ex. SOPHOS, " The *spam* economy: the convergence *spam* and virus threats ", mai 2005, disponible sur : http://www.sophos.com/whitepapers/Sophos_*spam*-economy_wpus.pdf ; « Les virus et le *spam*, ce qu'il faut savoir », spéc. p. 37, disponible sur : http://mirror.sweon.net/madchat/vxdevl/library/Les%20virus%20et%20le%20*spam*%20-%20ce%20qu%27il%20faut%20savoir.pdf.
[248] Le propriétaire de la machine expéditrice des *spams* sera identifié grâce à son adresse IP.
[249] À titre d'exemple, le virus Netsky qui se propage par *e-mail*, se présente sous la forme d'une pièce jointe à un message. Une fois exécuté, Netsky sera lancé à chaque démarrage de *Windows* et recherchera, dans le carnet d'adresses et sur les fichiers de l'ordinateur infecté, toutes les adresses électroniques pouvant être collectées. À l'aide d'un logiciel de messagerie, ce virus pourra ainsi se diffuser automatiquement à ces dernières (SOPHOS, *Security threat Report*, 2009, disponible sur :

malicieux dont le simple fait de cliquer dessus déclenchera l'exécution d'un *malware* [250]. Pour encourager les internautes à ouvrir les *e-mails* contenant des virus dommageables, les « spammeurs » utilisent souvent des évènements d'actualité [251] ou les noms de célébrités [252] ou encore d'hommes politiques dont les faits relatés éveilleront la curiosité des destinataires de ces messages.

b. Le *spamming*, vecteur d'escroqueries

105. Le *spam* véhicule d'arnaques en tout genre. Parmi les différentes catégories de *spams* recensées, MCAFEE, l'un des leaders mondiaux en matière de fourniture de solutions de sécurité informatique, rapporte que les *spams* peuvent contenir différents types de contenus trompeurs, certains sont relatifs à des crédits (par exemple, un *e-mail* qui promettrait de l'argent, des crédits ou chercherait à exploiter la solvabilité du destinataire du message), d'autres font la publicité pour des sites *Web* proposant de faux diplômes, d'autres encore tentent de vendre, à des prix très attractifs, des licences, des copies de logiciels piratées ou encore de faux produits pharmaceutiques, des compléments alimentaires, des produits promettant un amaigrissement rapide ou des produits comme des sacs ou des bijoux contrefaits, etc. [253]. À titre d'exemple, on peut encore citer les *spams* boursiers dont la croissance a été très importante entre 2005 et 2006 et qui portent sur des titres dont le cours

http://www.sophos.com/sophos/docs/eng/marketing_material/sophos-security-threat-report-jan-2009-na.pdf). – Même en l'absence de pièce jointe, la simple consultation d'un *e-mail* peut provoquer le déclenchement d'un script caché dont l'exécution permettra d'envoyer des *spams* à toutes les adresses électroniques présentes dans les fichiers de l'ordinateur infecté. Tel est le cas par exemple du virus « Bublleboy ».

[250] La campagne présidentielle de Barack OBAMA aux États-Unis a fait l'objet de plusieurs campagnes de *spams* dont les *e-mails* envoyés contenaient des liens vers des sites malveillants. En septembre 2008, SOPHOS rapportait qu'un *e-mail* contenait un lien vers une vidéo pornographique du candidat au poste présidentiel américain et dont la visualisation déclenchait l'installation d'un logiciel malveillant. En novembre 2008, à la suite de la victoire présidentielle d'OBAMA, une autre attaque de *malware* via des *spams* a été opérée en invitant les destinataires de ces messages à cliquer sur un lien pour voir une vidéo de la victoire du président. En réalité, la visite de ce site *Web* permettait de voler les informations contenues dans l'ordinateur de la victime et de les envoyer à un serveur à Kiev en Ukraine (v. *Security threat Report*, 2009, rapport préc.).

[251] En 2008, les « spammeurs » ont exploité divers faits d'actualité afin d'inciter les destinataires à ouvrir des logiciels malveillants : l'hypothétique intervention américaine en Iran, l'élection américaine ou encore les jeux olympiques (BITDEFENDER, *Rapport sur l'état des e-menaces*, 16 janv. 2009, disponible sur : www.bitdefender.fr/site/News/pdfDescription/922.pdf).

[252] Selon une étude de MCAFEE, les cinq célébrités les plus dangereuses du Cyberespace en 2010 sont l'actrice Cameron DIAZ en première position, suivie des actrices Julia ROBERTS et Jessica BIEL puis du mannequin Gisele BÜNDCHEN et enfin en cinquième position, l'acteur Brad PITT (" McAfee Most Dangerous Celebrities ", 19 août 2010, disponible sur : http://www.globalsecuritymag.fr/McAfee-nomme-Cameron-Diaz,20100819,19029.html).

[253] À cette liste, on peut également ajouter l'arnaque dont est victime le nouveau réseau social *Ping* qui, dès sa mise sur le marché, a été envahi de *spams* dont certains d'entre eux tentaient de convaincre les utilisateurs qu'ils recevraient un iPhone gratuit s'ils répondaient à des sondages en ligne (« À peine le nouveau service Ping de Apple lancé, les spammeurs l'inondent d'arnaques sur iPhone », art. préc.). – De même, SOPHOS avait repéré, l'été dernier, une nouvelle escroquerie au faux sondage (*scam*) qui circulait sur le réseau *Facebook* (« Une nouvelle escroquerie sur Facebook propose un faux bouton "Je n'aime pas" », 16 août 2010, disponible sur : http://www.sophos.fr/pressoffice/news/articles/2010/08/facebook-dislike.html.

est très bas [254]. Cette technique consiste à recourir à des mécanismes de fraudes et artifices [255] pour faire monter artificiellement le cours d'une action en s'assurant ainsi une plus-value substantielle sur une durée de temps limitée [256]. Le principe est le suivant : le fraudeur achète un grand nombre d'action ou de titres d'une société quelconque, le plus souvent, qui ne valent que quelques centimes (*pennies-stocks*) et crée une demande artificielle en vue de les revendre à un prix anormalement gonflé. L'attaquant entreprend alors une campagne d'envois massifs de *spams* vers des millions de destinataires, vantant les qualités de l'action afin d'inciter les destinataires à investir fortement grâce à divers prétextes (la rumeur d'une fusion avec une société puissante, par exemple). L'achat de cette action par quelques milliers de victimes entraîne une hausse importante de son cours à la suite de laquelle le « spammeur » revendra rapidement ses actions (« *dump* »), encaissant ainsi une importante plus-value au détriment des investisseurs qui subiront de fortes pertes suite à la chute du titre [257]. Plus récemment, SOPHOS a constaté, au troisième trimestre 2010, une multitude d'arnaques circulant sur *Facebook*, créées par les « spammeurs » afin de leur rapporter de l'argent à partir de sondages en ligne [258].

106. La connivence entre *spamming* et *phishing*. Empruntant aux artifices utilisés par le *phishing* [259], le « spammeur » envoie de faux courriers électroniques en usurpant l'identité d'un organisme financier ou d'un site commercial connu afin de leur donner toutes les apparences d'un *e-mail* authentique [260]. Les *spams* envoyés peuvent alors notamment

[254] Les *spams* boursiers sont également désignés par l'expression « *pump and dump* » qui signifie littéralement « glonfler et jeter » ou encore « *Stock dump* » ou « *Hype and Dump Manipulation* ».
[255] Pour une étude générale sur les manipulations des cours de l'action et les méthodes utilisées, v. par ex. Rajesh K. AGGARWAL et Guojun WU, " Stock market manipulations", *Journal of Business*, vol. 79, n° 4, p. 1915 et s. (2006). – Kevin C. BARTELS, " " Click Here to Buy the Next Microsoft ": The Penny Stock Rules, Online Microcap Fraud, and the Unwary Investor ", *Indiana Law Journal*, vol. 75, n° 1, p. 353 et s.
[256] À titre d'exemple, pour lutter contre cette forme de *spam*, la SEC (*Securities Exchange Commission*) a suspendu le cours de 35 titres suite à des manipulations via une campagne de spams. Cela a permis à la société Apparel Manufacturing Associates, Inc. (APPM) de réaliser une opération très rentable puisqu'elle a pu acheter un volume important d'action à 0,06 $ pour quelques jours plus tard les revendre à 0,45 $. V. : *SEC Suspends Trading Of 35 Companies Touted In Spam Email Campaigns*, disponible sur: http://www.sec.gov/news/press/2007/2007-34.htm. ; Marc REES, Spam financier : suspension sanction pour 35 titres boursiers, 13 mars 2007, http://www.pcinpact.com/actu/news/35209-SEC-Bourse-cours.htm.
[257] Le processus inverse existe également, le « *Short and distort* », qui consiste à profiter d'une baisse du cours d'une action provoquée artificiellement en raison de la divulgation de rumeurs mensongères et négatives.
[258] SOPHOS, « Classement trimestriel des douze principaux pays relayeurs de *spams* : la France premier émetteur européen », art. préc.
[259] Sur cette technique, v. Philippe BELLOIR, « La répression pénale du " phishing " », *RLDI* janv. 2006, n° 349, p. 30 et s. – Éric A. CAPRIOLI, « Le phishing saisi par le droit », art. préc. – Frédéric DUFLOT, « " Phishing " : les dessous de la contrefaçon », art. préc. – Romain V. GOLA, « Usurpation de l'identité sur l'internet : aspects de droit pénal comparé », *RLDI* déc. 2009, n° 1839, p. 65. – Guillaume JAHAN, « Personal Data Privacy and Security Act : combattre le détournement de données personnelles sur internet », *Gaz. Pal*. 20 oct. 2005, 2, doctr., p. 3269 et s. – Jean-Sébastien MARIEZ, « Un premier pas vers la mise en place d'un dispositif pertinent de lutte contre l'usurpation d'identité sur internet ? », *RLDI* nov. 2008, p. 65 et s. – David PERE et David FOREST, « L'arsenal répressif du phishing », *D.* 2006, chron. préc. – V. ég. OCDE, *Document exploratoire sur le vol d'identité en ligne*, préc.
[260] Selon une étude menée au second semestre 2009, les trois entités qui ont été le plus usurpées sont *PayPal*, *eBay et HSBC* (BITDEFENDER, Communiqué de presse, 24 août 2010, disponible sur : http://www.editions-

demander au destinataire de confirmer ses données identifiantes (informations financières et bancaires ou d'autres données nominatives, notamment le couplet identifiant/mot de passe) sur un faux site *Web*, copie conforme du site officiel, ou de se connecter au site mentionné dans l'*e-mail* dans le seul but d'infecter l'ordinateur du destinataire par le biais de logiciels malveillants [261]. Reposant sur une manipulation sociale *(social engineering*), les destinataires croient recevoir un message provenant d'un expéditeur connu ou de confiance et communique alors leurs données identifiantes sans méfiance [262]. Le *spamming* devient ainsi vecteur de messages frauduleux dont le contenu trompeur est destiné à faciliter le vol d'informations identifiantes.

107. L'escroquerie à la nigériane : l'exploitation des techniques du passé. Le *spamming* peut également prendre la forme d'un « *scam* », encore appelé escroquerie à la nigériane ou « fraude 419 », en référence à l'article 419 du Code pénal nigérian réprimant l'escroquerie. Il s'agit de l'une des escroqueries les plus anciennes qui a vu le jour au XVI[e] siècle sous le nom de « captive espagnole ». Cette technique consistait à envoyer une lettre en provenance d'une personnalité d'un pays africain qui prétendait connaître des difficultés avec la justice et qui cherchait de l'aide pour transférer ses fonds à l'étranger contre une part de sa fortune. S'inspirant de cette méthode très ancienne, le « spammeur » envoie un message dans lequel il se présente comme l'héritier d'un riche notable africain récemment décédé et prétexte que ce dernier aurait déposé, à son intention, des millions de dollars sur un

profil.eu/EP/RessourcesSiteProfil/Communiques/Rapport%20BitDefender%20sur%20l%E2%80%99%C3%A9tat%20des%20e-menaces%20au%20premier%20semestre%202010.pdf). – En 2010, certains « spammeurs » ont envoyé des *e-mails* faisant croire qu'ils provenaient légitimement du FAI FREE (Marc JACOB, « Nouvelle campagne de *spams* qui vise les clients de Free », août 2010, disponible sur : http://www.globalsecuritymag.fr/Nouvelle-campagne-de-spams-qui,20100831,19236.html), de *Visa MasterCard* (« Le *spam* de la semaine : Visa MasterCard », oct. 2010, disponible sur : http://www.globalsecuritymag.fr/Le-spam-de-la-semaine-Visa,20101031,20376.html) ou encore de *Microsoft* (« Le *spam* de la semaine touche tous les opérateurs d'un coup », novembre 2010, disponible sur : http://www.globalsecuritymag.fr/Le-Spam-de-la-semaine-touche-tous,20101109,20515.html).

[261] AVIRA, une société éditrice de solutions de sécurité informatique, rapportait en 2009 l'existence de *spams* prétendant contenir de nouveaux paramètres pour le service de messagerie. Certains de ces *spams*, qui donnaient l'impression de provenir de l'assistance du fournisseur de service de messagerie, contenaient en réalité en pièce jointe un logiciel malveillant. D'autres renvoyaient vers un site *Web* sur lequel on retrouvait l'aspect d'O*utlook Web Access* et sur lequel ce logiciel malveillant pouvait apparemment être téléchargé (« Un *spam* renvoie à un logiciel malveillant au lieu de paramètres email », 15 oct. 2009, disponible sur : http://row.avira.com/fr/actualites_sur_la_securite/spam_malveillant.html).

[262] SOPHOS a rapporté que cette tendance était apparue dans l'exploitation des réseaux sociaux et consistait pour les « spammeurs » à se faire passer pour des amis *Facebook.* Abusant ainsi de la confiance des destinataires, les « spammeurs » parvenaient à voler leurs noms d'utilisateur ainsi que leurs mots de passe pour ensuite bombarder d'*e-mails* les amis et membres de la famille de ces victimes (*Rapport sur les menaces à la sécurité*, rapport préc., spéc. p. 2 et s.). SOPHOS a également noté, au troisième trimestre 2010, une hausse du *spam* diffusé sur les réseaux sociaux comme *Twitter* ou *Facebook* et comportant des arnaques qui visaient notamment à inciter les utilisateurs à répondre à un sondage en ligne s'ils souhaitaient voir une photo ou une vidéo pornographique (« Classement trimestriel des douze principaux pays relayeurs de *spam* : la France premier émetteur européen », art. préc.).

compte bancaire [263]. Pour procéder au transfert de ces fonds, le « spammeur » s'en remet alors aux services du destinataire du message en le persuadant qu'il a besoin des coordonnées de son compte bancaire pour procéder au virement en échange d'un pourcentage substantiel sur cette somme. Les destinataires les plus crédules qui répondront au message permettront aux délinquants de réaliser leurs opérations, soit en effectuant l'ensemble des échanges en ligne, soit en les persuadant de le rejoindre dans son pays avec la somme en liquide. Dans le premier cas, après avoir récupéré les coordonnées bancaires de l'interlocuteur, ils vident à distance le compte de la victime ; dans le second, une fois sur le sol étranger, cette dernière est dépossédée de ses biens et de ses papiers d'identité.

*

* * *

108. Retracer les étapes du processus d'envois des *spams* a permis de prendre conscience des dangers qui pèsent sur les données nominatives, en particulier sur les adresses électroniques. Afin d'éviter que les « spammeurs » ne puissent les collecter aisément, il est essentiel que les titulaires adoptent une attitude vigilante chaque fois qu'ils les communiqueront en ligne. À défaut, ils deviendront les nouvelles cibles des « spammeurs » et s'exposeront à la réception de messages non sollicités. Les divers procédés auxquels ont recours les « spammeurs » démontrent l'agressivité et la dangerosité croissante du *spamming*, en particulier, au regard des techniques de plus en plus sophistiquées utilisées [264] ou encore de son association à des pratiques tout aussi illicites. Cette évolution du *spamming* vers des formes toujours plus malveillantes justifie impérativement la mise en place d'un système capable de protéger efficacement les « spammés » et leurs données nominatives.

[263] Cette technique représentait 21% du *spam* en janvier 2010 (SYMANTEC, *State of Spam & Phishnig*, n° 38, févr. 2010, disponible sur : http://eval.symantec.com/mktginfo/enterprise/other_resources/b-state_of_spam_and_phishing_report_02-2010.en-us.pdf).

[264] Le Laboratoire BITDEFENDER a découvert un schéma d'envoi de *spams* qui se révèle d'une complexité « byzantine », selon ses termes. Lorsque les utilisateurs essaient de cliquer pour visualiser une vidéo, ces derniers sont incités à télécharger un « media player » qui est en réalité le code malveillant « Backdoor.Edunet.E », et qui utilise les ordinateurs de victimes comme plateforme d'envoi de commandes à une série de serveurs de *mails*. Ces serveurs, qui appartiennent principalement aux domaines < .edu > et < .mil > correspondant respectivement aux organismes éducatifs et militaires, sont utilisés comme relais pour propager du *spam* (Communiqué de presse, 8 avril 2008, disponible sur : http://www.editions-profil.eu/EP/RessourcesSiteProfil/Communiques/Alerte%20du%20080408.pdf).

SECTION II. L'ÉCHEC D'UNE RÉPONSE EXCLUSIVEMENT TECHNIQUE

109. Alors que les services de messagerie électronique étaient conçus initialement comme un moyen fiable, rapide et économique pour communiquer des informations, la technicité et la dangerosité du *spamming* ont largement contribué à ternir leur image. Ces services sont en effet devenus incapables de garantir l'envoi quasi instantané de messages ou d'assurer leur réception et leur consultation en toute tranquillité. La lutte engagée contre le *spamming* doit alors s'efforcer de renforcer la sécurité et la fiabilité de ces services et plus largement des services de l'internet afin de retrouver la confiance des internautes. À cette fin, il est indispensable de mettre en place des solutions techniques capables, à la fois d'assurer la réception d'*e-mails* légitimes, mais aussi de bloquer les messages non sollicités. Cet objectif constitue néanmoins un véritable défi technique dès lors que les « spammeurs » s'évertuent à trouver sans cesse de nouveaux stratagèmes pour contourner les filtres anti-*spam*. Nous verrons en effet que l'évolution perpétuelle du *spamming* rend les dispositifs techniques de protection nettement insuffisants (§ 1.). Plus encore, il sera constaté que les failles des nouvelles technologies de communication peuvent servir involontairement au développement du *spamming* (§ 2.)

§ 1. L'INSUFFISANCE DES DISPOSITIFS TECHNIQUES DE PROTECTION

110. Quel que soit le dispositif choisi, son efficacité sera évaluée au regard de son aptitude à restaurer la confiance des internautes à l'égard des services de messagerie électronique [265]. Concrètement, il s'agira de vérifier si le procédé mis en place permet de garantir aux utilisateurs de ces services une utilisation normale de leurs boîtes électroniques. En effet, pour être considéré comme efficace, celui-ci devra en particulier démontrer sa capacité à les prémunir, non seulement contre tout risque de perte ou de blocage des *e-mails* sollicités, mais également contre l'encombrement de leurs messageries par des courriers indésirables, l'objectif étant d'assurer un flux des messages entrants et sortants fluide. Au regard de ces critères d'évaluation, il sera démontré que le recours aux filtres anti-*spam* offre des résultats trop aléatoires pour faire preuve d'une réelle efficacité (A.) que les *HoneyPots* ne permettront pas de surmonter (B.). Cette analyse se conclura toutefois sur une note positive, les techniques d'authentification se présentant comme un palliatif prometteur (C.).

[265] En effet, rappelons que la technique du *spamming* repose essentiellement sur un usage abusif du courrier électronique.

A. LES TECHNIQUES DE FILTRAGE, UN OUTIL ALEATOIRE

111. L'évolution des formats. Pour contourner les filtres anti-*spam*, les « spammeurs » ont imaginé toute sorte de stratagème en recourant notamment à divers formats des messages expédiés. Détrônant le *spam* par texte, le « *spam* image », apparu en 2006, avait pour particularité d'insérer le *spam* dans une image attachée au message et de ne plus le faire apparaître dans le corps du message lui-même. Cette technique a connu à ses débuts un vif succès qui s'expliquait à cette époque par l'existence de solutions anti-*spam* limitées à une analyse textuelle des messages. Mais l'apparition progressive de filtres de plus en plus performants a contraint les « spammeurs » à innover. Au cours de l'année 2007, de nouvelles formes de *spam* ont vu le jour, comme le *spam* « lien-image » [266] ou encore le « *spam* PDF » ou le « *spam* Excel » [267]. Puis, ce fut au tour du *spam* MP3 de faire son apparition [268]. Ces exemples mettent en évidence que la lutte contre le *spamming* s'inscrit dans un mouvement perpétuel d'attaques et de contre-attaques rythmé au gré des évolutions technologique même si l'évolution des supports du *spam* tend à revenir à des techniques plus élémentaires et plus simples d'utilisation [269].

112. Au cours de cette étude, nous constaterons que malgré le perfectionnement des filtres anti-*spams* destinés à détecter et à bloquer instantanément un grand nombre de messages non sollicités, les « spammeurs » redoublent d'imagination pour les contourner. Ainsi, les techniques de filtrage visant à automatiser la suppression des *spams* en fonction de son origine (1.) ou de son contenu (2.) se révèleront inefficaces, tout comme le test de *Turing*, une méthode de filtrage originale (3.).

[266] Technique qui consistait à ce que le message ne contienne qu'un lien renvoyant vers une image stockée sur un serveur en ligne laquelle n'est donc pas passée au travers des filtres traditionnels de contenu.
[267] L'image envoyée par le « spammeur » n'est pas dans le message mais dans un fichier attaché au format PDF ou Excel.
[268] Le principe consiste à enregistrer un message publicitaire au format MP3, de lui donner le nom d'une chanson puis de l'envoyer en masse par *e-mail* grâce un réseau de PC zombies.
[269] Une étude réalisée entre janvier et juin 2009 par BITDEFENDER a révélé une résurgence du *spam*-texte, qui a atteint 80 % au cours de cette période, contre 70% à la même période en 2008. Quant au *spam*-image, celui-ci a augmenté de 150% depuis le premier semestre 2008. Cette étude rapporte que « [l]*es images sont incorporées dans des spams imitant des newsletters au format HTML, ces images téléchargeables font partie de la stratégie développée par les spammeurs pour d'une part inciter les utilisateurs à accepter des images généralement bloquées par les clients de messagerie, et d'autre part contourner autant que possible les filtres anti-spam en modifiant légèrement la palette de couleurs de l'image* », disponible sur : http://www.globalsecuritymag.fr/Etude-semestrielle-BitDefender-sur,20090826,12125.html).

1. L'inefficacité des filtrages programmés en fonction de l'origine des messages

113. Ces techniques ont toutes pour caractéristique commune de filtrer les messages selon l'identification de leur émetteur à partir de listes constituées d'expéditeurs connus et classés par catégorie. Si l'émetteur est reconnu comme « spammeur », il sera répertorié dans une liste noire (a.). Au contraire, s'il est identifié comme un expéditeur de confiance, ce dernier sera inscrit sur une liste blanche (b.). Enfin, si l'identité de l'expéditeur est inconnue mais semble douteuse, son courrier sera temporairement bloqué sur une liste grise (c.).

a. Les listes noires, une technique aux multiples failles

114. Il existe deux catégories de liste noire (*blacklist*), l'une regroupant les adresses électroniques et/ou les domaines des « spammeurs » et l'autre, les adresses IP des serveurs de « spammeurs » déjà répertoriés comme tels [270].

115. Les listes noires d'adresses électroniques et/ou de domaines de « spammeurs ». Cette technique consiste à enregistrer dans une base de données l'ensemble des adresses électroniques et/ou noms de domaine d'émetteurs identifiés comme « spammeurs » [271]. L'élaboration de cette liste permet ainsi au serveur de messagerie de reconnaître et de refuser tout nouveau message provenant de ces adresses ou domaines. En pratique, ce procédé est extrêmement contraignant dans la mesure où il impose de mettre constamment à jour les listes auprès d'une base de données disponible sur l'internet et qui centralise des listes d'expéditeurs bloqués, elle-même devant être très souvent mise à jour. Malgré une actualisation systématique, il s'avère presque impossible de faire évoluer leur contenu au rythme de progression des « spammeurs ». De nouvelles adresses sont en effet continuellement créées et leur durée de vie est généralement limitée à celle de la campagne

[270] À l'issue d'une étude publiée en décembre 2009 par l'ENISA, l'agence européenne chargée de la sécurité des réseaux et de l'information, et portant sur les mesures anti-*spam* utilisées par les FAI européens, il apparaît que l'élaboration de listes noires constitue la méthode anti-*spam* la plus fréquemment utilisée et ce, quelle que soit l'importance de ces fournisseurs. Ce type de liste représente en effet 90% de l'ensemble des mesures anti-*spam* utilisées, dépassant ainsi largement les listes grises (55%) et les listes blanches (37%) (*What are the Measures Used by European Providers to Reduce the Amount of Spam Received by Their Customers ?*, déc. 2009, spéc. p. 32 et s., disponible sur : http://www.enisa.europa.eu/act/res/other-areas/anti-spam-measures).

[271] L'organisation non gouvernementale internationale, *SPAMHAUS PROJET*, a élaboré, par exemple, une liste des dix principaux « spammeurs » de la planète (v. « The World's Worst Spammers », mai 2011, préc.). Elle a également dressé une liste connue sous l'acronyme « ROSKO » (*Register of Known Spam Operations*), qui répertorie les « spammeurs » identifiés comme les plus menaçants et qui ont été exclus plus de trois fois des services de leur FAI. Pas moins de 140 personnes ou groupes spécialisés dans l'envoi de *spams* y sont dénombrés (v. le site de *Spamhaus Project* disponible sur : http://www.spamhaus.org/rokso/). – Sur le rôle de cette organisation à l'échelon international, v. : *infra* : n° 527

de *spams*, celle-ci n'excédant rarement quelques jours. En raison de ces changements perpétuels, les listes noires atteignent ainsi très vite des dimensions titanesques, extrêmement difficiles à gérer. Par ailleurs, il convient de noter que la constitution de ces listes peut avoir des effets pervers si le « spammeur » venait à utiliser des adresses usurpées. Dans ce cas de figure, les conséquences seraient lourdes pour les victimes puisque leur classification en tant que « spammeurs » entraînerait un blocage systématique de l'ensemble des messages qu'ils transmettraient à partir de leurs adresses électroniques.

116. Les listes noires d'adresses IP des serveurs de « spammeurs » connus. En raison d'un changement régulier de serveur, les adresses IP changent elles aussi ponctuellement, ce qui limite l'effectivité dans le temps de ces listes noires puisque seuls les envois émis depuis une même adresse IP peuvent être bloqués. Leur portée s'essouffle ainsi dans la mesure où il est nécessaire de les mettre en permanence à jour manuellement. Enfin, elles se révèlent impuissantes contre les *spams* fulgurants utilisant des PC zombies et engendrent des risques accrus de faux positifs [272], ce qui est problématique puisque la désinscription d'une adresse légitime répertoriée par erreur dans cette liste noire est souvent très longue.

b. Les listes banches, facteur de blocage des flux d'*e-mails*

117. Le blocage des *e-mails* légitimes mais inconnus. En complément des listes noires, les listes blanches (*whitelist*) consistent à dresser une liste des noms de domaine, adresses électroniques ou adresses IP provenant d'expéditeurs identifiés comme fiables. Si cette technique permet d'éviter de classer à tort des messages légitimes comme des *spams* (faux positifs) et inversement, de répertorier des *spams* dans la catégorie des messages légitimes (faux négatifs), sa mise en œuvre se révèle très lourde. En effet, pour passer le filtre anti-*spam*, le message devra subir le processus de confirmation qui risque de ralentir la communication et provoquer certaines irritations de la part des expéditeurs qui se savent légitimes. Plus grave, ce processus bloquera des *e-mails* légitimes provenant de nouvelles sources et donc pas encore répertoriés comme légitimes.

[272] V. Glossaire.

c. Les listes grises, frein à une communication rapide des *e-mails*

118. Ralentissement des échanges. Les listes grises (*greylists*) constituent l'échelon intermédiaire entre les listes noires et les listes blanches. Cette technique anti-*spam* est basée sur le blocage temporaire des courriers électroniques reçus. L'analyse d'un triplet de données, composé de l'adresse IP du serveur émetteur et des adresses respectives de l'émetteur et de l'expéditeur du message, permettra de décider du blocage éventuel du message. Dans le cas où l'une de ces trois données est inconnue, l'*e-mail* sera temporairement placé sur une liste grise. Un code d'erreur sera transmis au serveur de messagerie d'émission du message lui indiquant de renvoyer à nouveau ce message après l'écoulement d'un certain délai. Si le serveur de messagerie le renvoie correctement, le triplet de données sera alors validé et placé en liste blanche. L'envoi de futurs messages utilisant ce triplet sera à l'avenir accepté, pendant un certain temps, sans nouvelle attente de confirmation. Correctement configurée, cette technique présente l'avantage de ne générer pratiquement aucun faux positif et de réduire efficacement le nombre de *spams* acceptés sur un serveur. Toutefois, l'inconvénient majeur tient au temps de vérification du message qui ralentit sa transmission et peut se révéler gênant lorsqu'il est urgent.

2. L'inefficacité des filtrages programmés en fonction du contenu des messages

119. À la différence des techniques précédentes, ce type de filtrage analyse le contenu du message selon trois mécanismes distincts : le filtrage par mots-clés (a.), le filtrage à heuristique (b.) et enfin le filtrage Bayesien (c.), chacun présentant des faiblesses plus ou moins importantes.

a. Le filtrage par mots-clés, un procédé élémentaire inopérant

120. Un filtrage inefficace face aux multiples parades des « spammeurs ». Cette méthode consiste à dresser une liste de mots fréquemment employés par les « spammeurs » (« viagra », « porno », etc.) et à les classer comme interdits. Son efficacité se révèle toutefois très limitée face aux multiples parades auxquelles ont recours les « spammeurs ». En effet, pour contourner ces filtres, ces derniers déguisent les mots considérés comme les plus utilisés dans les *spams* en les déclinant sous des formes variées. Cette technique, appelée « *hashbusting* », vise à créer des textes dynamiques en introduisant de légères variations dans le *spam* originel afin de masquer la similarité des contenus envoyés. Il peut s'agir

d'insérer des espaces, des caractères spéciaux entre les lettres, d'ajouter des chaînes de caractères aléatoires à la fin du texte, ou encore d'inverser certaines lettres dans un mot, de substituer des lettres par des chiffres de forme ressemblante : un zéro remplaçant un « o », un « 1 » à la place d'un « I », un « 5 » pour un « S » ... Par exemple, le terme « viagra » peut être écrit de multiples façons : « vIagra », « v.i.a.g.r.a », « Vi@gra » ou encore « v i a g r a », etc. Les « spammeurs » ont également recours à des messages invisibles en utilisant des lettres écrites en blanc sur fond blanc pour les dissimuler ou une police réduite ou un texte coloré pour masquer l'arrière plan. Un même *spam* pourra dès lors apparaître sous des variantes aussi nombreuses que le sont les destinataires. Cette multitude de combinaisons rend donc très difficile, voire dans certains cas, impossible d'envisager l'ensemble des formes que peut prendre un même mot et en tout état de cause, contraint à comparer un large échantillon de messages avant de pouvoir l'identifier comme étant un *spam*.

121. Un risque important de faux négatifs et de faux positifs. Le risque de faux négatifs est particulièrement important dans la mesure où les *spams* ressemblent de plus en plus aux messages légitimes. Quant aux risques de faux positifs, les résultats ne sont guère plus convaincants. En effet, imaginons qu'un médecin, après une consultation, envoie un *e-mail* à son patient dans lequel il utilise le mot « viagra », la présence de ce seul mot dans le message suffira à le bloquer alors même que dans ce contexte, il n'aurait aucune raison de l'être.

b. Le filtrage à heuristique, un procédé plus élaboré mais toujours fragile

122. Processus de mise en œuvre. Plus évoluée que la méthode précédente, cette technique consiste à rechercher, dans le contenu du message, certaines caractéristiques habituelles du *spam*. Le principe n'est pas ici de bloquer tous les *e-mails* contenant un mot figurant sur la liste des « interdits » mais d'attribuer un « score » global au contenu du message selon divers tests destinés à relever l'existence d'indices susceptibles de détecter la présence de *spams*. Parmi les tests possibles, il s'agit de vérifier la validité des adresses de l'expéditeur considérées comme suspectes en contrôlant si l'un des serveurs expéditeurs appartiendrait à une liste noire, de rechercher la présence dans le corps du message d'un mot figurant sur la liste des « interdits » ou des tournures de phrases classiquement rencontrées dans les *spams*, etc. En pratique, plusieurs indices peuvent concourir à suspecter la présence de *spams*. Il en est ainsi lorsque l'objet du message contient par exemple des fautes

d'orthographe [273], fait référence à un sujet d'actualité, une célébrité ou un homme politique. C'est également le cas lorsque le message renvoie à des contenus à caractère pornographique ou à l'un des domaines suivants : médical (perte de poids), financier (gain d'argent), vente de produits miracles [274], etc. D'autres indices peuvent également éveillés des soupçons, notamment lorsque l'adresse est composée de séquences numériques incrémentées automatiquement du type : « sophz2044@hotmail.fr, sophz2045@hotmail.fr, sophz2046@hotmail.fr, etc., ou encore lorsque le champ « *from* » de l'en-tête du message contient des adresses similaires à celles de l'expéditeur concerné (attaque dictionnaire). Chaque test contribue à déterminer un score final. À l'issue de l'évaluation, en fonction d'un certain seuil défini par l'utilisateur, le score obtenu indiquera une probabilité plus ou moins forte que ce message sera du *spam*.

123. Inconvénient : un risque important de faux négatifs. En termes d'efficacité, cette méthode impose la mobilisation de beaucoup de ressources machines et les risques de faux négatifs sont relativement importants, les « spammeurs » s'efforçant notamment de masquer les mots clés grâce à différentes techniques comme l'ARCII Art (*American Standard Code for Information Interchange*) [275] en reproduisant des formes à partir d'une suite de caractères qui formera à son tour un message non reconnu par les filtres.

c. Le filtrage Bayesien, un procédé d'analyse subtil mais d'effectivité limitée

124. Fonctionnement. Basée également sur le contenu et les en-têtes du message, cette méthode consiste à attribuer une probabilité à un mot ou à une combinaison de mots-clés contenus dans les courriers selon une étude statistique et un calcul de probabilités. Le principe repose sur le classement des messages reçus dans une base de données selon qu'ils sont reconnus comme des *spams* ou considérés comme des messages légitimes (« *ham* »). Une fois que la base « *Spam*/*Ham* » est constituée, il est attribué à chaque mot une probabilité à partir de la comptabilisation du nombre d'occurrences d'un terme présent dans chaque catégorie de messages. L'objectif de cette technique est d'apprendre à distinguer la terminologie utilisée par les « spammeurs » du vocabulaire légitime. Par exemple, si le mot « *pharmacy* » apparaît quarante fois dans des *spams* contre cinq fois dans des messages

[273] « Bravo, vous avez ga-gné ».
[274] L'un des indicateurs de la présence de *spam* peut être le recours à des expressions typiques telles que « Perdez 7 kilos en 7 jours » ou le fait des promesses grotesques comme celles de faire fortune sans bouger de chez vous, ou de perdre 15 kilos en une semaine.
[275] Pour un exemple de *Spam* ARTII Art, v. « Spam : Ascii Art et Spam », disponible sur : http://assiste.com.free.fr/p/*spam*/ascii_art_et_*spam*.html#.

légitimes, il existe de fortes chances pour que ce mot appartienne au langage des « spammeurs » et sera alors classé dans la liste des mots interdits. Chaque fois qu'un nouveau message apparaît, le filtre calculera sa probabilité de « spamicité » en combinant les différents résultats obtenus pour chaque mot. Il sera alors possible de déterminer la probabilité globale qu'un message appartienne ou non à la catégorie de *spam*. Pour cela, l'anti-*spam* incrémentera une « jauge » qui déclenchera le classement du message dans la catégorie des *spams* lorsque celle-ci dépassera une certaine valeur.

125. Atouts. Cette méthode présente l'avantage de soumettre tous les mots présents dans le courrier électronique au test. Le calcul de la probabilité globale de « spamicité » d'un message évite ainsi de bloquer tous les messages qui contiendraient certains mots suspects et permet, de cette manière, de résoudre le problème que pose le filtrage à heuristique [276]. Cette méthode autodidacte et personnalisée qui s'adapte rapidement aux évolutions des parades utilisées par les « spammeurs », permet de modifier les règles d'attribution des scores selon des besoins spécifiques. Dans le cas où les « spammeurs » veulent par exemple contourner le filtre en déguisant certains mots (par exemple, « 5ex » au lieu de « sex » ou CaSh » au lieu de « cash »), la mise à jour de la base de données de *spam* en incluant ces mots masqués permettra ainsi de les reconnaître et de détecter leur présence dans les prochains messages électroniques.

126. Faiblesses. Si ces filtres sont particulièrement efficaces lorsqu'ils sont utilisés à titre individuel ou dans un environnement de travail de taille réduite, relevant d'un même secteur d'activité, leur efficacité devient limitée dès lors qu'elle est utilisée de façon collective. En effet, s'appuyant sur un apprentissage du vocabulaire légitime et illégitime, cette méthode devient rapidement impraticable lorsque les individus du groupe considéré utilisent un vocabulaire très varié. En outre, l'efficacité de ce procédé nécessite une phase d'apprentissage préalable des mots ou signes interdits qui peut être relativement longue et surtout risque de rendre des résultats sans réelle certitude. Toutefois, l'inconvénient majeur est le risque de faux négatif puisque les « spammeurs » s'ingénient à trouver des stratagèmes destinés à altérer l'efficacité de ce type de filtre. Parmi les techniques utilisées, la plus efficace consiste pour le « spammeur » à placer dans le message une grande quantité de textes provenant notamment de faits tirés de l'actualité afin de noyer les parties indésirables de l'*e-mail* et tromper ainsi le filtre.

[276] V. *supra* : n° 122.

3. Le test de *Turing*, un risque important de faux positifs

127. Fonctionnement. Cette technique consiste à envoyer un message automatique qui demande à l'expéditeur du message de fournir une confirmation de retour de leurs adresses électroniques. L'objectif est de vérifier si l'expéditeur est un individu ou si le message a été généré par une machine. Pour effectuer cette vérification, il sera demandé au prétendu expéditeur du courrier de relever un « challenge » qu'une machine ne saurait réaliser. Celui-ci est qualifié de « classique » lorsqu'il s'agit de reproduire une série de lettres et de chiffres et de « cognitif » lorsqu'il s'agit de répondre à une question, simplissime pour l'humain, mais impossible pour un robot [277]. Si l'émetteur transmet une réponse correcte, son origine humaine est avérée. Dans cette hypothèse, son adresse sera automatiquement placée en liste blanche et son courrier sera sorti de la file d'attente et transmis à l'expéditeur. En revanche, en cas de réponse incorrecte ou inexistante, l'émetteur sera suspecté de recourir, soit à une adresse véritable mais usurpée, soit à une adresse qui n'existe pas soit encore à celle d'un robot. Dans ces trois dernières hypothèses, l'*e-mail* restera en quarantaine et ne sera pas délivré. Enfin, si l'adresse est réelle et correspond à celle d'un « spammeur », l'avalanche d'énigmes à résoudre empêchera toute action de sa part.

128. Inconvénients : les faux positifs. Ce type de filtre risque de bloquer certains *e-mails* légitimes, notamment des *newsletters* ou des messages relatifs à des mises à jour de certains produits si une société n'a pas prévu une personne physique chargée de répondre au test [278]. Par ailleurs, la lenteur de réception du premier envoi peut être gênante lorsque la correspondance est urgente et l'exposer ainsi à un risque supplémentaire de perte de sa confidentialité. Enfin, parmi les inconvénients les plus mineurs, ce test peut risquer de déplaire à certains expéditeurs qui peuvent y voir à son égard une certaine méfiance des destinataires [279].

129. En définitive, l'exposé des différentes techniques de filtrage actuelles révèle qu'aucune d'entre elles ne peut s'imposer comme un dispositif de protection infaillible restaurant la confiance des *internautes* envers les services de messagerie. Si les filtres les plus efficaces restent encore ceux paramétrés par l'utilisateur final en personne, seuls les

[277] Pour des exemples de ces « challenges », v. MAILINBLACK, « *Spam* – État de l'art », Livre Blanc, 2006, spéc. p. 14, disponible sur : http://assiste.com.free.fr/ftp/livre_blanc_le_*spam*.pdf.
[278] Parmi les différentes évolutions du *spam*, SOPHOS a par exemple noté en 2008 une nouvelle tendance qui consiste à reproduire les modèles et *design* de *newsletters* légitimes pour envoyer des *spams* (*Security threat Report*, 2009, rapport préc.).
[279] Pour une vue complète de cette technique, v. « Anti-spam - Outils à base de tests de Turing », disponible sur : http://assiste.com.free.fr/p/*spam*/anti-*spam*_et_test_de_turing.html#ref_Captcha.

initiés semblent, à ce jour prêts, à investir du temps et de l'argent dans un outil qui nécessite un paramétrage quasi quotidien.

B. LES *HONEYPOTS*, UNE TECHNIQUE SURANNEE

130. Fonctionnement. Le *HoneyPot*, littéralement « pot de miel », désigne dans le langage informatique un programme volontairement vulnérable destiné à tromper les « spammeurs » pour les attirer et les piéger. Il peut s'agir notamment de créer une adresse électronique spécialement conçue pour ne recevoir que du *spam* et de l'inclure de façon visible dans de nombreuses pages de sites *Web* pour servir d'appât. Cette adresse sera, de cette façon, rapidement détectée par les robots des « spammeurs » et collectée par ces derniers. À la réception des premiers *spams*, le système de filtrage détecte le moment de la collecte puis sauvegarde l'adresse IP et l'adresse électronique utilisées. L'autre stratagème consiste à utiliser un serveur de messagerie, en apparence très vulnérable car peu sécurisé, et qui servira en réalité à enregistrer les informations relatives aux « spammeurs » qui s'y attaqueront.

131. Inconvénients. Si cette technique a connu un certain succès à ses débuts lorsque le *spamming* ne représentait encore qu'une simple gêne, celle-ci semble aujourd'hui dépassée par l'ampleur du phénomène. Pour contourner cette technique, les « spammeurs » ont en effet recours à des textes dynamiques [280] qui neutralisent l'efficacité du filtre et ralentissent la détection des *spams*.

C. LES TECHNIQUES BASEES SUR L'AUTHENTIFICATION, UN PALLIATIF PROMETTEUR

132. Dans la mesure où les méthodes de filtrage ont largement démontré leurs limites, de nouvelles techniques ont été mises au point pour surmonter les failles du processus d'authentification du protocole de communication SMTP. Des systèmes ont été développés afin d'authentifier les émetteurs à partir de l'adresse IP contenue dans l'en-tête du courrier et de vérifier si elle correspond à un nom de domaine connu et autorisé à envoyer des messages. Schématiquement, le principe consiste à extraire le domaine de l'adresse de l'émetteur et à vérifier dans le DNS si le serveur expéditeur qui tente de transmettre ce message, figure dans la liste des serveurs de messagerie autorisés. Si c'est le cas, le message

[280] Pour une description de cette technique, v. *supra* : n° 120.

est accepté sinon il est supprimé, refusé ou fait l'objet de tests plus approfondis. Trois techniques peuvent être recensées. Les deux premières, le *Sender Policy Framework* (SPF) et le *Sender* ID visent à vérifier l'authentification de l'adresse IP de la machine de l'expéditeur tandis que la troisième, le *Domain Keys Identified Mail*, repose sur la cryptographie, un procédé qui s'appuie sur le chiffrement des données afin de conserver leur confidentialité et leur authenticité.

133. Les processus de fonctionnement du SPF et de Sender ID. Il s'agit d'une technologie qui vise à authentifier le nom de domaine de l'expéditeur du message reçu par un serveur destinataire. Le serveur de réception récupère le nom de domaine de l'adresse électronique indiquée dans le champ « *Mail From* » figurant dans l'en-tête du message. À titre d'exemple, si l'adresse est sophmil@hotmail.com, le serveur de réception saisit le nom de domaine <hotmail.com> et interroge ensuite le serveur DNS de ce nom de domaine pour vérifier s'il est autorisé à envoyer des courriers électroniques [281]. Lorsque le serveur est interrogé, le protocole suggère au destinataire du message de rejeter systématiquement les *e-mails* qui proviennent prétendument d'un domaine ou bien d'accepter ces messages, tout en avertissant le destinataire final de sa potentielle illégitimité.

134. *Domain Keys Identified Mail* (DKIM). Mise au point par Yahoo ! et *Sendmail*, cette technologie, basée sur la cryptographie est destinée à lutter contre la falsification des adresses électroniques (*spoofing*) et consiste à authentifier le nom de domaine de l'expéditeur d'un courrier électronique ainsi que l'intégrité de ce message afin de s'assurer que les en-têtes et le contenu du message n'aient pas été modifiés en cours de transmission [282]. Au niveau du serveur expéditeur, une clé publique sera ajoutée au serveur DNS du domaine identifié et des clés privées seront stockées sur le serveur d'envoi légitime. Lors de l'expédition d'un message, le serveur d'envoi utilise une clé privée pour signer électroniquement le message, cette signature sera alors insérée dans l'en-tête du message. Une fois le message envoyé, le serveur destinataire récupère le nom de domaine et la signature de l'*e-mail* puis la clé publique auprès du serveur DNS de l'expéditeur présumé grâce à laquelle il vérifiera si elle correspond à la clé privée de l'*e-mail*. Si le message ne

[281] Schématiquement, ces deux techniques se différencient au regard de l'interprétation des données recueillies auprès des DNS. Toutefois, nous ne rentrerons pas dans ces détails trop techniques dans la mesure où ils ne présentent pas d'apport essentiel pour notre recherche. – Pour de plus amples informations sur le fonctionnement de Sender ID, V. MICROSOF, « Sender ID Framework », 2006, disponible sur : http://download.microsoft.com/download/d/f/0/df0b1f68-a05e-4949-be0a-26d6787da6af/fr_sidf.pdf et http://www.microsoft.com/mscorp/safety/technologies/senderid/default.mspx.

[282] V. YAHOO! Media Relations, « *Sendmail* and Yahoo ! Mail collaborate to develop and deploy Domainkeys », disponible sur : http://docs.yahoo.com/docs/pr/release1143.html. – Pour plus d'informations sur le fonctionnement de *DomainKeys*, v. YAHOO! « Prouver et sécuriser l'identité des expéditeurs », disponible sur : http://fr.docs.yahoo.com/mail/spamguard_domainkeys.html.

contient pas de signature ou si celle-ci n'est pas valide, le serveur du destinataire peut rejeter l'*e-mail* ou le délivrer au destinataire final en lui notifiant une possible usurpation d'identité. De cette manière, *DomainKeys* certifie que les contenus du message n'ont pas été altérés lors de leur transmission.

135. Le cryptage, une technique intéressante mais pas infaillible. La technique du cryptage semble être un outil de lutte efficace contre le *spamming*, l'authentification des *e-mails* révélant l'identification de l'expéditeur du courrier. De cette manière, elle aurait un réel effet dissuasif sur les « spammeurs » puisque le destinataire du message pourrait facilement rapporter la preuve de l'identité du « spammeur ». Cette dernière est d'ailleurs encouragée par différents organismes travaillant sur la protection des données personnelles, tels que la Commission nationale de l'informatique et des libertés (CNIL) [283], l'organe consultatif chargé de la protection des données à caractère personnel (Groupe « article 29 »), encore appelé « G29 », en référence à l'article 29 de la directive n° 95/46/CE du 24 octobre 1995 [284] par lequel il a été institué et regroupant les représentants de vingt-sept autorités indépendantes chargées de la protection des données nationales [285] ou encore le Comité des ministres du Conseil de l'Europe [286]. Néanmoins, il est possible de douter de l'efficacité et de la mise en œuvre de cette technique par l'utilisateur lambda qui généralement ne la maîtrise pas. Par ailleurs, la signature du message n'est pas sans faille puisque le « spammeur » peut enregistrer pour une somme modique un domaine, créer les bons enregistrements dans le DNS et transmettre des messages signés. Par ailleurs, il est également à signaler que certains « spammeurs » ont utilisé le procédé de *DomainKeys* pour rendre leur messages plus légitimes [287], diminuant ainsi l'effectivité de ce procédé.

[283] Autorité administrative indépendante instituée par la loi n° 78-17 du 6 janvier 1978 relative à l'Informatique, aux fichiers et aux Libertés (J.O. du 7 janvier 1978, p. 227 et s. et rectificatif, J.O. du 25 janvier 1978) qui a pour mission essentielle de protéger la vie privée et les libertés dans le monde numérique, v. son site disponible sur : http://www.cnil.fr. – Pour une description de ses pouvoirs, v. *infra* : n° 247 et s.

[284] Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, J.O.U.E. n° L. 281 du 23 novembre 1995, p. 31 et s.

[285] Sur le rôle « majeur » du G29 dans la protection des données à caractère personnel à l'échelle européenne mais aussi mondiale, v. Sophie NERBONNE, « Le Groupe de l'article 29 est-il en mesure de s'imposer comme le régulateur des régulateurs par ses prises de position ? », *Legicom* 2009/1, n° 42, p. 37 et s.

[286] Le Comité des ministres aux États membres sur la protection de la vie privée sur Internet a notamment recommandé l'utilisation des « *technologies appropriées et* [des] *technologies disponibles, de préférence celles faisant l'objet d'une certification* » et d' « *informer l'utilisateur des moyens techniques qu'il peut utiliser licitement pour diminuer les risques concernant la sécurité des données et des communications, tels que le cryptage et les signatures électroniques légalement disponibles* » (Recommandation n° R (99) 5 préc., spéc. p. 4).

[287] Dennis FISHER, " Scammers Exploit DomainKeys Anti-phishing Weapon ", 29 nov. 2004, disponible sur : http://www.eweek.com/article2/0,1759,1732576,00.asp.

§ 2. LES NOUVELLES TECHNOLOGIES DE COMMUNICATION AU SERVICE DES « SPAMMEURS »

136. Victime de son succès, l'internet a créé involontairement un environnement propice aux développements d'actes malveillants. Les « spammeurs » ont su tirer avantage des nouvelles technologies de communication ou profiter de certaines de leurs faiblesses pour agir de façon dissimilée. En particulier, l'absence d'identification obligatoire de l'expéditeur dont souffre le protocole de communication SMTP laisse une large porte ouverte à la falsification de l'adresse électronique de l'expéditeur (*spoofing*) mais aussi à l'exploitation de serveurs de messagerie non sécurisés ou mal configurés ou encore à des postes infectés de virus. Face à ces artifices, le « spammé » sera le plus souvent confronté à des difficultés techniques tenant d'une part, au suivi de parcours des *spams* (A.) et d'autre part, au traçage des flux financiers (B.).

A. LES DIFFICULTES TECHNIQUES DE SUIVI DU PARCOURS DES *SPAMS*

137. Le *spoofing* ou l'usurpation du nom de domaine. Le *spamming* repose sur un usage abusif du courrier électronique [288]. Pour le comprendre, il convient de rappeler brièvement le fonctionnement de transmission du courrier électronique. L'envoi d'*e-mails* est notamment régi par le protocole SMTP. Lorsque l'expéditeur transmet un courrier électronique, son ordinateur le transfère par SMTP au *Mail Transfert Agent* (MTA), un serveur de messagerie chargé du transport du message, jusqu'au MTA destinataire. Le message est ainsi relayé de MTA en MTA jusqu'au MTA final, le *Mail Delivery Agent* (MDA), en charge de la gestion des boîtes aux lettres. À la réception de ce courrier, le serveur de messagerie du destinataire le sauvegarde jusqu'à ce que le destinataire le récupère *via* les protocoles POP3 ou IMAP, protocoles permettant de relever les messages pour leur lecture. Dans ce schéma de transmission, le processus d'authentification SMTP n'exige aucune authentification préalable permettant de s'assurer de l'identité de l'expéditeur, l'échange de courriers électroniques reposant sur un système de confiance. Les « spammeurs » exploitent ainsi abusivement cette vulnérabilité du fonctionnement du système de messagerie électronique pour dissimuler leur identité – adresses électroniques usurpées voire inexistantes, spécialement créées à cet effet – afin d'empêcher leur traçabilité [289]. Diverses conséquences plus ou moins lourdes peuvent se

[288] Sur le fonctionnement et l'échange d'*e-mail*, v. not. Florence BITAN, *Courrier Électronique*, *J.-Cl. Communication*, Fasc. 4740, 2006, spéc. n^os^ 2-3. – David E. SORKIN, " Unsolicited Commercial E-Mail and the Telephone Consumer Protection Act of 1991 ", 45 *Buffalo Law Review* 1001, spéc. pp. 1005-1006 (1997).

[289] Déjà en 2004, la FTC dénonçait que plus de 90% des *spams* se révélaient intraçables (*A CAN-SPAM Informant Reward System – A Report to Congress*, sept. 2004, spéc. p. 11, disponible sur : http://www.ftc.gov/reports/rewardsys/040916rewardsysrpt.pdf).

répercuter sur les « spammés ». Celles-ci peuvent notamment être désastreuses lorsque le « spammeur » utilise l'adresse électronique d'un tiers. En effet, l'ensemble des *e-mails,* qui ne pourra pas être adressé à un destinataire, sera renvoyé à l'adresse électronique falsifiée depuis laquelle les courriers électroniques ont été adressés. Dans cette hypothèse, la redirection vers cette adresse d'expédition risque de créer un engorgement voire une saturation de la boîte de réception de cet utilisateur innocent. Sans usurper l'identité d'un tiers, les « spammeurs » peuvent également avoir recours à des adresses de retour générées de façon aléatoire. La falsification des informations de routage empêche de la sorte toute localisation puisque ce procédé permet de bloquer la traçabilité des serveurs de messages par lesquels le *spam* a transité.

138. L'anonymat de la connexion à l'internet. Plusieurs possibilités existent pour se connecter à l'internet de façon telle que la trace de l'auteur de la connexion est rendue impossible. Le « spammeur » peut en effet se connecter à l'internet grâce à une adresse de réseau qui ne peut pas être reliée à un individu ou à un emplacement physique. Outre l'envoi de messages par l'intermédiaire des PC zombies [290], cette hypothèse couvre une connexion à l'internet grâce à une connexion WIFI utilisée à l'insu de son utilisateur légitime, à un cyber-café ou aux réseaux des campus de certaines universités qui ne requièrent aucune authentification préalable et permet ainsi l'envoi de courriers électroniques de façon anonyme. Les « spammeurs » peuvent aussi acheter à un FAI un accès vagabond utilisant des noms faux et des méthodes de paiement intraçables.

139. L'anonymat des messages. Le recours à un *remailer* permet à un expéditeur d'envoyer des messages grâce à la suppression de toutes les informations identifiantes destinées à déterminer l'origine du message (notamment, les informations contenues dans l'en-tête du message, telles que le champ « *from* » contenant l'adresse du « spammeur », l'adresse IP, etc.) et qui sont remplacées par la mention « *anonymous* » avant de renvoyer au destinataire le message devenu anonyme.

140. *Open relay* (relais ouvert). Le transfert de courrier électronique est opéré le plus souvent *via* l'intermédiaire de plusieurs serveurs d'*e-mails*. Ces intermédiaires, appelés relais, interviennent dans l'acheminement des messages vers leur destinataire. Certains d'entre eux, mal configurés (*open relay*), acceptent et transfèrent le courrier électronique provenant de n'importe quel expéditeur. Ils deviennent ainsi la cible privilégiée des « spammeurs » dans la mesure où cette faille technique leur permet d'envoyer des millions

[290] Sur cette technique d'envoi, v. *supra* : n° 104.

de *spams* depuis ces ordinateurs. Par exemple, un « spammeur » établi aux États-Unis pourrait envoyer des *e-mails via* un relais ouvert localisé en Russie, ce qui lui permettrait ainsi de les faire apparaître comme provenant de la Russie.

B. LES DIFFICULTES TECHNIQUES DE TRAÇAGE DES FLUX FINANCIERS

141. Selon la Commission fédérale du commerce américaine (FTC) chargée de l'application d'une série de lois fédérales relative à la protection des consommateurs et à la concurrence, la technique d'investigation qui s'avère la plus efficace pour identifier les « spammeurs » repose sur le suivi de la trace financière de l'argent parce que derrière nombre de *spams* frauduleux, il existe une personne qui bénéficie au final financièrement de la transmission de *spams*. Ainsi, la réception de fonds peut permettre d'identifier et de tracer le délinquant. Cette technique consiste à suivre la trace des flux financiers vers cette personne qui mènera au « spammeur » avec qui elle est associée. Dans de nombreux cas, des indices peuvent être trouvés dans le message électronique liant l'expéditeur au produit offert. Toutefois, cette technique présente certaines limites dans la mesure où les « spammeurs » ont souvent recours à de multiples méthodes de paiement (utilisation de comptes de carte de crédit volés, des paiements en *cash*,…) destinées à anéantir les efforts de traçage du flux d'argent. En effet, pour rendre plus complexe leur traçabilité, les délinquants feront appel à des mules qui joueront le rôle d'intermédiaire entre la victime et l'escroc en échange du versement d'un pourcentage de la somme gagnée. La difficulté s'accroît encore lorsque les « spammeurs » recourent à des paradis fiscaux [291].

*

* * *

142. Le recensement de certaines des techniques anti-*spam* a permis de constater les réelles difficultés qu'elles rencontrent pour lutter efficacement contre cette pratique. Dans ces circonstances, le recours simultané à plusieurs techniques de filtrage est fréquent afin de compenser les faiblesses de chacune d'elles lorsqu'elles sont utilisées de façon indépendante [292]. Toutefois, cette superposition des techniques n'est pas sans conséquence

[291] FTC, *A CAN-SPAM Informant Reward System*, rapport préc., spéc. pp. 14-15.
[292] Par exemple, le logiciel *open source SpamAssassin* utilise, à la différence des autres filtres anti-*spam*, une combinaison de techniques de filtrage : une analyse du contenu selon la méthode de pondération, des listes

puisque, non seulement elle ralentit la vitesse de délivrance des messages mais impose également la mobilisation d'importantes ressources machines, ce qui représente une charge importante sur le réseau [293]. De leur côté, les techniques d'authentification participent activement à l'amélioration de l'identification des expéditeurs légitimes pour les domaines protégés mais restent toutefois insuffisantes au regard des diverses techniques utilisées par les « spammeurs » pour effacer toutes traces de leur activité et empêcher leur suivi.

noires et un algorithme de BAYES qui « apprend » à reconnaître les nouveaux *spams* à partir d'anciens messages non sollicités, disponible sur : http://spamassassin.apache.org/.

[293] Les listes grises imposent de traiter davantage de connexions SMTP, par exemple.

CONCLUSION DU CHAPITRE 1

143. Une lutte technique insuffisante. La lutte anti-*spam* apparaît comme une véritable course à l'armement technique dont tirent avantageusement profit les « spammeurs ». La réussite de leurs activités dépend en effet de leur capacité à constamment innover pour devancer la contre-offensive technique. Les diverses évolutions et perfectionnements du *spamming*, tant au stade de la collecte des données qu'à celui de l'envoi des *spams*, attestent de la supériorité technique des « spammeurs ». Pour atteindre leur objectif, ces derniers exploitent la moindre faille des systèmes informatiques et optimisent leurs opérations en dissimulant leur identité [294] au moyen de divers stratagèmes. Pour leur part, les techniciens ont œuvré à la mise en place de dispositifs de sécurité toujours plus sophistiqués pour tenter de répondre à ces attaques croissantes qui tendent à se complexifier. Toutefois, les résultats obtenus grâce aux filtres anti-*spam* démontrent clairement leur manque de fiabilité. De leur côté, les FAI comme les internautes doivent mettre à profit les différents outils techniques qui sont à leur disposition. Dans le cas précis du grand public, il est essentiel de promouvoir une meilleure sensibilisation des internautes au sujet des risques inhérents à la divulgation de leurs données sur le réseau et de leur fournir une information plus complète quant aux logiciels disponibles sur le marché.

144. En définitive, s'il apparaît que les disposifs de protection technique doivent jouer un rôle afin d'enrayer la persistance du *spamming*, ces derniers constituent toutefois une réponse manifestement insuffisante pour appréhender ce phénomène dans son ensemble. En particulier, il convient de souligner que le *spamming* engendre également certains problèmes économiques et sociaux qui s'étendent au-delà du royaume des bits et des octets. Dans un objectif permanent d'efficacité, la lutte anti-*spam* doit dès lors s'engager à la fois sur un front technique mais également juridique [295]. Les orientations législatives doivent venir au soutien de la réponse technique pour répondre aux défis socio-économiques qu'implique le *spamming*.

[294] V. *supra* : n° 136.
[295] En faveur d'une intervention nécessaire du gouvernement pour soutenir les mesures techniques, v. not. Michael W. CARROLL, " Garbage In: Emerging Media and Regulation of Unsolicited Commercial Solicitations ", 11 *Berkeley Tech. L.J.* 233 (1996).

CHAPITRE SECOND : LES DÉFIS SOCIO-ÉCONOMIQUES

145. Le *spamming*, au cœur d'oppositions difficilement conciliables. Face aux multiples menaces que véhicule cette pratique, il est non seulement impératif de trouver une réponse juridique capable d'assurer le bon fonctionnement des services de l'internet, notamment de courrier électronique, mais également de protéger les adresses électroniques, matière première du *spamming*. Toutefois, cette quête de protection se révèle être un véritable défi pour les législateurs, confrontés à une fracture entre les intérêts des « spammeurs » et les préoccupations des « spammés ». D'une part, les enjeux économiques qui s'attachent aux données nominatives incitent les « spammeurs » à mener des opérations de collectes et traitements massifs à la plus grande inquiétude des titulaires de données qui semblent de plus en plus désarmés face aux traitements massifs de ces dernières. D'autre part, alors que les premiers tentent de légitimer leur activité au nom de la liberté d'expression commerciale, les seconds souhaitent ne pas être importunés pas des courriers électroniques non sollicités. La question de la protection des « spammés » face au *spamming* s'insère donc dans un contexte conflictuel où les motivations économiques et justification des « spammeurs » (Section I.) alimentent une inquiétude sociale croissante (Section II.)

SECTION I : LES MOTIVATIONS ÉCONOMIQUES ET JUSTIFICATION AU SOUTIEN DU *SPAMMING*

146. Techniquement, l'envoi de *spams* est nécessairement précédé de la collecte de données, en particulier, des adresses électroniques, puisqu'elles permettant d'identifier les futurs destinataires [296]. La réussite de cette opération dépend donc de la capacité des « spammeurs » à rassembler une quantité importante de telles données. La source potentielle de profits que représentent ces identifiants numériques motive dès lors leur collecte intensive (§ 1.). Par ailleurs, le *spamming* s'inscrivant généralement dans une perspective publicitaire, c'est essentiellement sur le fondement de la liberté d'expression commerciale qu'ont porté les revendications des « spammeurs », notamment américains, pour tenter de justifier leur activité (§ 2.).

§ 1. LES ADRESSES ÉLECTRONIQUES, UNE SOURCE POTENTIELLE DE PROFITS

147. Le recoupement des données nominatives, une activité au cœur du commerce électronique personnalisé. La CNIL ayant très tôt pris conscience de l'enjeu économique des identifiants numériques, a souligné dans son rapport d'activité pour l'année 1996 que l'identification des internautes constitue un impératif majeur dans le commerce électronique et particulièrement pour la prospection par voie électronique [297]. Ainsi, comme l'observe le professeur Jean FRAYSSINET, « *les informations relatives aux consommateurs*

[296] Pour les besoins de notre démonstration, nous limiterons notre étude aux adresses électroniques puisque ce sont les données les plus couramment utilisées par les « spammeurs ». Toutefois, ces développements couvrent plus largement la collecte d'autres données nominatives telles que les numéros de téléphone dans le cadre des *spams* mobile.

[297] CNIL, *Rapport d'activité 1996*, n° 17, Doc. fr., 1997, spéc. pp. 90-91 (« *C'est la montée en puissance de l'Internet commercial qui stimule abondamment les pratiques d'identification des Internautes, dans le but de meilleure connaissance et de fidélisation de la clientèle des services en ligne* »). – Quelques années auparavant, la CNIL reconnaissait déjà « *la valeur marchande de l'information nominative* », et constatait que « [l]*es entreprises et les administrations prennent de plus en plus conscience de la valeur marchande des informations qu'elles détiennent sur les personnes. Il est vrai qu'aujourd'hui le commerce d'adresses est devenu une activité économique à part entière et que des entreprises se consacrent exclusivement à la vente et à la location de fichiers* » (*Rapport d'activité* 1989, n° 10, Doc. fr., 1990, spéc. p. 9). – V. ég. Georges CHATILLON, *Les données personnelles : enjeux juridiques et perspectives : rapport au Premier ministre sur la transposition en droit français de la directive numéro 95-46*, rapport préc., spéc. p. 2 (constatant que : « [l]*es bases de données personnelles constituent* […] *désormais un marché à part entière. Leur constitution et leur traitement sont l'élément principal de la valeur ajoutée produite par un grand nombre d'entreprises de services : vente par correspondance, agences de relations publiques, agences de casting, conseils en recrutement, entreprise de travail temporaire* »). – Reprenant cette idée, le professeur Michel DUPUIS constatait également que « *les données relatives aux personnes ont donc fini par acquérir une valeur marchande* » (« La Vie privée à l'épreuve de l'internet : quelques aspects nouveaux », *RJPF* 2001, n° 12). – De même, Jacques FAUVET, ancien président de la CNIL, présentant à la presse le 18e rapport d'activité de la Commission (CNIL, *Rapport d'activité 1997*, n° 18, Doc. fr., 1998), soulignait que « *l'exigence de liberté des citoyens* », prédominante il y a vingt ans, avait été remplacée par *« un impératif économique de libre circulation des données*. Il ajoutait que celles-ci étaient désormais « *devenues des marchandises qu'on vend, achète, sous-traite ou enrichit* » (Allocution prononcée à Paris le 8 juillet 1998, disponible sur : http://www.juriscom.net/uni/mem/03/biblio.html).

sont devenues un bien précieux, coûteux, recherché, échangé sur un véritable marché nouveau. Elles constituent souvent la vraie valeur économique, capitalistique, de nombre d'entreprises et spécialement des créateurs de sites et de portails sur l'Internet, des fournisseurs d'accès. Leur croisement et traitement servent de levier au développement du commerce électronique et du nouveau marketing » [298]. La reconnaissance d'une valeur économique potentielle des données à caractère personnel et de leur utilité commerciale est donc incontestable [299]. On assiste à une évolution des modes de *marketing* : au *marketing* de masse succède le « *marketing one to one* » [300] ou « *marketing direct* », fondé sur une offre individualisée [301]. La collecte d'informations identifiantes contribue à une meilleure connaissance des attentes des consommateurs. Grâce aux multiples recoupements possibles entre les diverses données collectées, les professionnels du *marketing* direct peuvent désormais proposer une offre plus personnalisée. Dans ces circonstances, la gestion de la relation client (« *Customer Relationship Management* » (CRM)) qui consiste à identifier les besoins et les comportements des clients devient donc essentielle [302] pour fidéliser les clients existants, les orienter vers de nouveaux produits en créant de nouveaux besoins (*marketing* incitatif) ou encore pour capter de nouveaux clients. Fondement de l'ensemble des opérations publicitaires de *marketing* direct, ces fichiers nominatifs présentent dès lors un grand intérêt pour les entreprises qui souhaitent mener une prospection « *intelligente et rentable* » [303], en se tournant vers le consommateur final afin de créer une relation « sur mesure ». En effet, la force de ce commerce personnalisé dépend de sa capacité à proposer une offre adaptée aux attentes et intérêts des consommateurs. À cette fin, les entreprises ont besoin de collecter un maximum d'informations nominatives sur les individus pour connaître leurs habitudes de

[298] Jean FRAYSSINET, « Nouvelles technologies de l'information et de la communication et protection des libertés des consommateurs », art. préc., spéc. p. 55 ; « La traçabilité des personnes sur l'internet, une possible menace pour les droits et libertés », art. préc., spéc. n° 10 p. 94 et n° 22, p. 103. – Sur la constitution des fichiers d'entreprises et leur utilisation, v. CNIL (organisée par), *23e conférence internationale des commissaires à la protection des données : Vie privée – Droits de l'homme* , 24-26 sept. 2001, Doc. fr., 2002, spéc. p. 407 et s., p. 472 et s., p. 491 et s.

[299] Pour une étude générale sur les différentes utilisation des données nominatives à des fins commerciales, v. not. Nathalie MALLET-POUJOL, Jean FRAYSSINET et al., « Exploitation économique des données personnelles et protection de la vie privée » *in Les nouvelles frontières de la vie privée, Legicom* 2009/2, n° 43, p. 69 et s.

[300] Martha ROGERS et Don PEPPERS, *Le One to One : valorisez votre capital client*, Les Éditions d'Organisation, coll. *Pratique du marketing direct*, Paris, 1997.

[301] Philippe LEMOINE, « Commerce électronique, marketing et liberté » *in* Pierre TABATONI (sous la dir.), *La protection de la vie privée dans la société de l'information*, P.U.F., 2000, p. 9 et s. – CNIL, *Rapport d'activité 1997*, rapport préc., spéc. pp. 117-118 (« *l'exploitation des données comportementales recueillies sur l'internaute permet-elle d'adapter, dans l'instant, la publicité utilise au profil de celui-ci.* […] *les cyberconsommateurs* […] *deviennent personnellement prospectées* »).

[302] Michel DUPUIS explique que les traces laissées par les internautes « *sont destinées à cerner la personnalité des individus, en dressant par regroupement leur profil psychologique puis en les classant selon des critères précis* […]. *Ces fichiers sont ensuite vendus à des producteurs de sites, des publicitaires en ligne ou des entreprises du commerce électronique. C'est grâce à ces informations que pourront être listés les destinataires d'offres publicitaires ciblées* » ou que s'afficheront « *de multiples bandeaux publicitaires lors de leur navigation sur le Net* » (« La Vie privée à l'épreuve de l'internet : quelques aspects nouveaux », art. préc.).

[303] Jean FRAYSSINET, « La traçabilité des personnes sur l'internet, une possible menace pour les droits et libertés », art. préc., spéc. n° 22, p. 103. – V. ég. Éric A. CAPRIOLI, « Commerce à distance sur l'Internet et protection des données à caractère », *Comm. com. électr.* févr. 2005, Étude 7, p. 24 et s., spéc. n^{os} 1-2.

consommation, leurs goûts, leur cadre familial, etc. Cette opération de collecte est largement facilitée grâce à la profusion des données nominatives que les internautes communiquent spontanément à l'occasion des diverses opérations réalisées en ligne [304]. Ainsi, l'adresse électronique, recoupée avec d'autres informations identifiantes communiquées par l'internaute, permet aux prospecteurs de faire transparaître une image de l'individu virtuel aussi proche que possible de la réalité tout en favorisant la création d'offres très ciblées [305]. Dans cette perspective, c'est donc l'aspect qualitatif qui prime : plus les profils sont affinés et complets, et plus les fichiers acquerront de la valeur. On comprend dès lors que le recoupement des données à caractère personnel puisse représenter une source de profits substantielle et qu'« *avec la numérisation des données, l'information sur la personne non seulement fait l'objet d'un traitement massif mais est devenue intégrante d'un marché* » [306].

148. Des outils techniques au service d'un commerce électronique personnalisé. Le perfectionnement des outils techniques offre désormais la possibilité de recourir à des logiciels spécialisés capables de stocker l'ensemble de ces données dans d'immenses bases de données à des fins d'analyse et d'exploitation les plus diverses [307]. Par recoupement des différentes traces informationnelles relatives à un même individu et collectées à l'occasion de ses multiples requêtes, il sera possible de dresser son profil comportemental d'achat et/ou de consommation (*profiling*) [308] et de connaître ses goûts, ses centres d'intérêt afin d'adapter avec précision et pertinence le message publicitaire en fonction de ce profil [309]. La personnalisation des offres publicitaires peut également être réalisée grâce à une autre technique qui consiste à évaluer les consommateurs, de façon

[304] V. *supra :* n° 83 et s.

[305] Certains ont ainsi vu dans l'informatique une « *dévoreuse d'identité, elle capte l'individu sous toutes ses facettes et porte au grand jour des aspects qu'il souhaiterait conserver secrets* » (Didier POUSSON, « L'identité informatisée » *in* Jacqueline POUSSON-PETIT (sous la dir.), *L'identité de la personne humaine – Étude de droit français et de droit comparé*, Bruylant, Bruxelles, 2002, p. 371 et s., spéc. pp. 373-374).

[306] Nathalie MALLET-POUJOL, « Appropriation de l'information : l'éternelle chimère », chron. préc., spéc. n° 16, p. 333.

[307] V. Jean FRAYSSINET, « Nouvelles technologies de l'information et de la communication et protection des libertés des consommateurs », art. préc., spéc. pp. 46-47 ; « *La traçabilité des personnes sur l'internet* », *Dr.et patr.* mai 2001, n° 93, p. 76 et s.

[308] Selon la CNIL, « [l]a *méthode des profils utilise la capacité de traitement de l'ordinateur, pour, au regard des caractéristiques définies a priori ou déterminées après une étude statistique, classer des individus et prendre des décisions à leur égard* » (*Dix ans d'informatique et libertés*, (préf. Jacques FAUVET), Economica, Paris, 1988, spéc. p. 46). La CNIL désigne cette technique sous l'appellation de « segmentation comportementale ». Concrètement, celle-ci « *permet de construire, au sein de la clientèle d'un établissement ou d'une entreprise, des classes homogènes de clients appelés segments, en fonction des éléments en possession de l'établissement et figurant dans les fichiers* […]. *Chaque client est rattaché à un segment dont l'ensemble des caractéristiques est connu. Chaque segment offre des possibilités particulières de placement des différents produits de l'établissement* » (*Rapport d'activité 1993*, n° 14, Doc. fr., 1994, spéc. p. 59 et s., spéc. p. 60). – Sur cette question, v. également Jean-Marc DINANT, Christophe LAZARO, Yves POUILLET, et al. (rapport présenté par), *L'application de la Convention 108 au mécanisme de profilage : Éléments de réflexion destinés au travail futur du Comité consultatif*, 24e réunion, 13-14 mars 2008, disponible sur : http://www.coe.int/t/dghl/standardsetting/dataprotection/Reports/CRID_Profilage_2008_fr.pdf.

[309] V. G29, Avis n° 2/2010 sur la publicité comportementale en ligne, 00909/10/FR, WP 171, disponible sur : http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_fr.pdf.

automatique et systématique, puis à les classer (*scoring*) afin d'adapter la publicité à leurs attentes et préférences. Enfin, le *data mining* ou extraction de données est un dispositif de prospective destiné à faciliter le travail des entreprises de *marketing* en anticipant les tendances à venir des consommateurs. À partir des données collectées et rassemblées, ce procédé permet de les trier par catégorie et de les analyser afin d'en extraire l'information décisive [310].

149. L'adresse électronique, l'identifiant indispensable et parfois suffisant à la prospection commerciale. Dans le domaine de la prospection commerciale, l'adresse électronique occupe une place essentielle et, pourrait-on même dire, indispensable puisque tout envoi commercial est subordonné à la collecte préalable des adresses électroniques. À l'instar de l'adresse postale, l'adresse électronique permet ainsi que cette offre personnalisée parvienne à la personne ciblée. L'enjeu de ce type de données est donc « *la contactabilité, ou la possibilité techniquement offerte à un tiers d'injecter un contenu informationnel (et notamment de la publicité) dans une boîte aux lettres ou sur un écran* » [311]. Les « spammeurs » ont bien compris cet enjeu : la possibilité d'envoyer des *spams* à travers le monde, de façon presque instantanée, et à un coût dérisoire [312] a fait de ce mode de prospection le moyen le plus rentable pour atteindre un public planétaire en un temps record. Si les adresses électroniques se trouvent au cœur de notre débat, c'est bien parce qu'elles sont la raison d'être du *spamming* [313]. En effet, plus les bases de données des « spammeurs » regroupant les adresses électroniques seront richement alimentées par ce type d'informations identifiantes, et plus ils parviendront à atteindre un nombre considérable de destinataires. L'enjeu économique des adresses électroniques devient dès lors incontestable. Contrairement au commerce personnalisé, il ne s'agit plus de séduire le destinataire en lui adressant des messages publicitaires adaptés à ses attentes mais de toucher un public le plus large possible. Ce type d'opérations publicitaires agressives et perturbatrices s'illustre tout particulièrement en matière de *spamming*. En effet, le succès de cette pratique dépend étroitement du volume d'adresses collectées : toute préoccupation tenant à l'aspect qualitatif de l'annonce publicitaire est la plupart du temps évincé au profit de son seul aspect quantitatif.

[310] Sur cette technique du *data mining*, v. *L'application de la Convention 108 au mécanisme de profilage*, rapport préc., spéc. p. 9 et s.
[311] Jean-Marc DINANT, *Rapport sur les lacunes de la Convention n°108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel face aux développements technologiques (Partie I)*, Strasbourg, 22e réunion, novembre 2010, T-PD-BUR(2010)09 (I) FINAL, spéc. p. 7, disponible sur : http://www.coe.int/t/dghl/standardsetting/dataprotection/CoE%20Lacunes%20de%20la%20Convention%20108%20Part%20I%20TPD.pdf.
[312] Sur ce mode de prospection particulièrement lucratif, v. *supra :* n° 8.
[313] V. *supra :* n° 83 et s.

§ 2. LE *SPAMMING* JUSTIFIÉ AU NOM DE LA LIBERTÉ D'EXPRESSION COMMERCIALE

150. L'échec de certaines tentatives de justification. Les « spammeurs », et tout particulièrement ceux localisés aux États-Unis, ne manquent pas d'imagination pour tenter de légitimer leur activité [314]. Parmi les moyens de défense avancés, ces derniers ont tenté de faire valoir, en vain, la doctrine américaine des installations essentielles (*essential facilities doctrine*), doctrine selon laquelle une entité qui contrôle une installation rare a une obligation d'y donner un accès raisonnable aux concurrents [315]. Leur argumentation consistait ainsi à soutenir que les FAI contrôlaient un équipement essentiel auquel ils avaient un droit d'accès raisonnable en tant que concurrents. Sans surprise, l'argument n'a pas convaincu les tribunaux [316] ; FAI et « spammeurs » ne pouvant être considérés comme tels. En effet, tandis que les FAI fournissent à leurs abonnés un accès à l'internet, certains « spammeurs » font la promotion de produits ou de services. Le « spammeur » apparaît ainsi davantage comme un utilisateur des services fournis par son FAI, services qui lui permettent notamment d'envoyer des messages publicitaires par le biais de courrier électronique. Les « spammeurs » se sont également défendus en qualifiant les FAI de service public (*public utility*), argument qui n'a cependant pas été plus persuasif. En effet, pour retenir la qualification de service public, il est notamment nécessaire que les FAI possèdent un bien ou un service de première nécessité (*essential good or service*) sur lequel le public a un droit légal d'exiger qu'il soit fourni sans discrimination. Or, cette condition ne peut être satisfaite en ce sens que la diffusion de messages publicitaires n'est pas subordonnée à la seule condition de disposer d'un accès à l'internet, celle-ci pouvant être réalisée par le biais d'autres canaux de communication, tels que la télévision, le courrier postal ou encore les journaux [317]. L'échec de ces arguments n'a toutefois pas découragé les « spammeurs ».

[314] L'origine du *spamming* provenant essentiellement des États-Unis, nous nous intéresserons spécialement aux arguments des « spammeurs » localisés aux États-Unis.

[315] *Restatement (Second) of Torts* § 259 (1995). – Pour plus de détails, v. Cathryn LE, Note, " How Have Internet Service Providers Beat Spammers ? ", 5 *Rich. J. L. & Tech.* 9 (1998).

[316] V. not. *Cyber Promotions, Inc. v. America Online, Inc*., 948 *F. Supp*. 456, spéc. 464 (E.D. Pa., Nov. 4, 1996).

[317] Pour des précisions sur cette qualification de service public, v. not. Cathryn LE, Note, " How Have Internet Service Providers Beat Spammers? ", art. préc., spéc. pp. 18-21 (deux hypothèses peuvent permettre de retenir la qualité d'acteur public : soit le FAI exerce une activité exclusivement publique, soit un fonctionnaire d'État a aidé ou a agi de concert avec un FAI dans la fourniture d'un service d'accès à l'internet au public, auquel cas ce fonctionnaire et ce FAI sont considérés comme des entités interdépendantes). – Pour un exemple de refus de qualification d'un FAI en service public, v. par ex. *Cyber Promotions, Inc. v. America Online, Inc*., 948 *F. Supp*. 456, aff. préc. (dans cette affaire, les juges ont constaté que ni l'une ni l'autre de ces conditions n'étaient vérifiées : pour le refus d'activité exclusivement publique, v. 948 *F. Supp*. 436, aff. préc., spéc. 442 et pour le refus d'interdépendance, v. *id*., spéc. 444-445). – V. ég. *CompuServe, Inc. v. Cyber Promotions, Inc.*, 962 *F. Supp*. 1015 (S.D. Ohio, Feb. 3,1997), préc., spéc. 1026-1027 (retenant que COMPUSERVE était un acteur privé).

151. La liberté d'expression commerciale, une justification *a priori* plus convaincante. La liberté d'expression commerciale est une composante dérivée de la liberté d'expression, principe de droit fondamental de toute société démocratique [318] et consacré par la jurisprudence américaine [319]. Dès lors que le *spamming* a pour finalité de promouvoir des produits ou services sur l'internet, cette pratique constitue à ce titre une forme d'expression commerciale [320]. En raison de l'importance consacrée à cette liberté [321], c'est essentiellement aux États-Unis que ce moyen de défense a été le plus vivement allégué, les « spammeurs » américains ayant vu dans l'absolutisme apparent du Premier amendement de la Constitution américaine une arme redoutable pour défier les lois anti-*spam*. En effet, toute loi anti-*spam* vise, par définition, à limiter la liberté d'expression commerciale et est par conséquent susceptible d'être défiée sur le terrain constitutionnel. Face à cet argument se pose la question de savoir si le discours commercial est protégé par le Premier amendement de la Constitution américaine au même titre que le discours non commercial (politique, religieux…). L'étude de certaines jurisprudences sélectionnées et retenues comme les plus

[318] En 1789, la liberté d'expression est inscrite dans les constitutions de part et d'autre de l'Atlantique. Le 17 septembre 1787, les États-Unis adoptent leur propre constitution, amendée pour la première fois le 25 septembre 1789. Dans un souci d'éviter toute dérive possible de la part du législateur, la vision américaine ne semble *a priori* admettre aucune restriction à la liberté de communication, « [l]*e Congrès ne* [pouvant] *prendre aucune loi* […] *restreignant la liberté d'expression* » et toute attitude contraire étant considérée comme anticonstitutionnelle (" *Congress shall make no law* […] *abridging the freedom of speech or of the press* " (*U.S. Const. amend.* I)). À l'inverse, le relativisme de la formulation française rime avec un certain interventionnisme étatique en permettant au législateur d'apporter certaines restrictions à son exercice. Héritage de la Révolution française, la liberté d'expression est consacrée pour la première fois à l'article 11 de la Déclaration des droits de l'Homme et du Citoyen (DDHC) du 26 août 1789 qui énonce que « *La libre communication des pensées et des opinions est un des droits les plus précieux de l'homme ; tout citoyen peut donc parler, écrire, imprimer librement sauf à répondre de l'abus de cette liberté dans les cas déterminés par la loi* ». Cette liberté de s'exprimer et de communiquer, consacrée comme un principe fondamental du droit français, est néanmoins limitée dans son exercice au respect d'un certain nombre d'obligations : « *Nul ne peut être inquiété pour ses opinions, même religieuses, pourvu que leurs manifestations ne troublent pas l'ordre public établi par la loi* » (Article 10 DDHC). (Sur ces deux approches, américaine qualifiée de « négative », le Premier amendement se limitant à interdire au législateur fédéral toute intervention, par opposition à celle existant en France, qualifiée de « positive », v. Laurent PECH, *Approches européenne et américaine de la liberté d'expression dans la société de l'information*, *J.-Cl. Communication*, Fasc. 1250, 2010, spéc. n^{os} 8-17 ; « Approches européenne et américaine de la liberté d'expression dans la société de l'information, *Comm. com. électr.* juill.-août 2004, Étude 20, p. 13 et s.).

[319] Parmi les juges de la Cour suprême des États-Unis, c'est sans doute le juge BRANDEIS qui, dans la décision *Whitney v/ People of state of California* (274 *U.S.* 357, spéc. 375-376 (1927)), a le mieux exprimé l'importance de la liberté d'expression dans le système démocratique américain. – De même, la jurisprudence de la Cour européenne des droits de l'homme énonce que : « *La liberté d'expression constitue l'un des fondements essentiels de* [la …] *société* [démocratique], *l'une des conditions primordiales de son progrès et de l'épanouissement de chacun* » (CEDH, 7 déc. 1976, requête n° 5493/72, (A-24, § 49). – En France, le juge constitutionnel, plus mesuré, a parlé de « *liberté fondamentale, d'autant plus précieuse que son exercice est l'une des garanties essentielles du respect des autres droits et libertés et de la souveraineté nationale* » (Cons. const., DC n° 84-181 du 11 octobre 1984, J.O. du 29 juillet 1984, p. 3200 et s., *Rec. const.*, p. 78, spéc. consid. n° 37). – Pour des précisions sur ce point, v. Laurent PECH, *Liberté d'expression : Aperçus de droit comparé*, fasc. préc., spéc. n^{os} 15-17.

[320] Le discours commercial a fait l'objet de nombreuses définitions jurisprudentielles. – Sur cette question, v. Ian J. SILVERBRAND, " Commercialspeech.com : ACPA and the First Amendment ", 12 *UCLA J.L. & Tech.*, Issue 1, 1 (2008), spéc. pp. 14-18 ; *Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n of New York*, 447 *U.S.* 557, spéc. 561 (June 20, 1980) (" *commercial speech, that is, expression related solely to the economic interests of the speaker and its audience* ").

[321] La Constitution américaine réserve en effet la première place à cette liberté. En revanche, c'est plutôt sur le fondement de la liberté du commerce et de l'industrie que les « spammeurs » français défendraient leur activité, en particulier sur l'un des aspects de cette liberté à savoir, la liberté d'entreprendre.

marquantes en la matière permettra de mesurer la place accordée à la liberté d'expression dans le discours commercial et l'intensité de sa protection lorsque celle-ci est invoquée pour légitimer la pratique du *spamming*. Nous verrons que la protection du discours commercial est, par principe, relative (A.) et que la liberté d'expression commerciale ne saurait, par conséquent, légitimer pleinement et de façon inconditionnelle l'activité des « spammeurs » tel que ces derniers le soutiennent (B.).

A. UNE PROTECTION RELATIVE DU DISCOURS COMMERCIAL

152. Rejet d'une conception absolutiste. Il est acquis que l'effectivité de la liberté d'expression, principe à valeur universelle [322], ne saurait être remise en cause selon la nature du mode de communication concerné. La Déclaration universelle des droits de l'homme adoptée en 1948, exclut toute restriction à cette liberté, quelque soit le moyen d'expression en cause [323]. De même, le Pacte international relatif aux droits civils et politiques adopté en 1966, anticipant les évolutions technologiques futures, précisait déjà clairement que chacun jouit de ce droit « *par tout autre moyen de son choix* » [324]. Il devient ainsi, avec l'évolution des nouvelles technologies, un principe fondateur du réseau Internet, dominé depuis sa création par « *la prépondérance d'une idéologie libérale aux parfums libertaires* » [325]. La portée de son exercice apparaît donc immense dès lors que celui-ci a vocation à s'appliquer à un moyen de communication universel comme l'est l'internet [326]. La généralité des termes du

[322] Sa consécration en tant principe à valeur universelle ne viendra que plus tardivement. Il faudra en effet attendre la fin de la seconde guerre mondiale pour que ce principe soit reconnu au niveau international puis européen et qu'il soit consacré comme un. L'ONU a voté en 1948 la Déclaration universelle des droits de l'homme : « *tout individu a droit à la liberté d'expression* […] *sans considérations de frontières* » (article 19). Le Pacte international relatif aux droits civils et politiques, adopté par l'Assemblée des Nations unies le 16 décembre1966, reconnaît également le caractère universel de ce principe : « *Toute personne a droit à la liberté d'expression* […] *sans considération de frontières* ». Au niveau européen, la Convention de sauvegarde des droits de l'homme et des libertés fondamentales du 4 novembre 1950 garantit également la liberté d'expression comme un droit de l'homme dont l'article 10 énonce que « *Toute personne a droit à la liberté d'expression* […] *sans qu'il puisse y avoir ingérence d'autorités publiques et sans considération de frontières* ». L'article 10.1 de la Convention européenne de sauvegarde des Droits de l'homme et des libertés fondamentales dispose : « *Toute personne a droit à la liberté d'expression. Ce droit comprend la liberté d'opinion et la liberté de recevoir ou de communiquer des informations ou des idées sans qu'il puisse y avoir ingérence d'autorités publiques et sans considération de frontière* ». L'article 11 de la charte fondamentale des droits de l'homme du 7 décembre 2000 dispose : « *1. Toute personne a droit à la liberté d'expression. Ce droit comprend la liberté d'opinion et la liberté de recevoir ou de communiquer des informations ou des idées sans qu'il puisse y avoir ingérence d'autorités publiques et sans considération de frontières. 2. La liberté des médias et leur pluralisme sont respectés* ».

[323] Art. 19.

[324] Art. 19, al. 2.

[325] Laurent PECH, « Approches européenne et américaine de la liberté d'expression dans la société de l'information », étude préc., spéc. n° 13.

[326] L'application du Premier amendement à l'internet présente toutefois certaines spécificités. – V. not. sur ce point, l'affaire *Reno v. ACLU* (521 *U.S.* 844 (June 26, 1997)) dans laquelle les juges ne considèrent pas l'internet comme « *un medium de même nature que la radio ou la télévision pour les fins d'application du Premier amendement* » ; il existerait une sorte de « *hiérarchie des médias au regard de l'application du Premier*

Premier amendement de la Constitution américaine semble plaider en ce sens puisqu'il enjoint le Congrès de ne pas légiférer dès lors que le texte proposé vise à entraver l'exercice de cette liberté : « *Le Congrès ne pourra prendre aucune loi* […] *restreignant la liberté d'expression* », toute attitude contraire étant considérée comme inconstitutionnelle [327]. Toutefois, si l'interprétation littérale du Premier amendement semble suggérer une approche absolutiste de la liberté d'expression, par opposition à l'approche française plus modérée [328], cette opposition doit être néanmoins tempérée. En effet, il convient de préciser que la Cour Suprême a toujours refusé de considérer les garanties accordées par la Constitution américaine comme absolues et a, en particulier, admis que le Premier amendement ne conférait pas à l'individu un droit absolu à s'exprimer [329]. En effet, tout en reconnaissant que la Constitution des États-Unis garantit cette forme d'expression, la Cour Suprême lui accorde un degré de protection inférieur à celui reconnu aux autres formes d'expression telles que le discours religieux ou politique[330]. Cette différence de protection résulte de l'attachement de la Cour Suprême à établir un équilibre entre la liberté de s'exprimer et les droits d'autrui ou l'intérêt public, ce qui rejoint au moins partiellement la lettre du texte français [331].

153. L'affaire *Rowan v. United States Post Office Dept.* Dans cette espèce, la Cour Suprême des États-Unis a refusé de reconnaître l'expression commerciale comme un

Amendement » (Karim BENYEKHLEF, « *ACLU v. Reno* : pour la reconnaissance d'un régime propre à l'Internet au regard de la liberté d'expression », *Lex Electronica*, vol. 3, n° 2, hiver 1997, disponible sur : http://www.lex-electronica.org/docs/articles_180.html). – En France, la transcription législative française de cette liberté s'est tout d'abord construite à partir de son support historique, la presse, avec l'adoption de la loi du 29 juillet 1881 sur la liberté de la presse qui affirme, en son article 1er, que : « *l'imprimerie et la presse sont libres* ». Pour sa part, l'article 1er de la loi n° 47-585 du 2 avril 1947 relative au statut des entreprises de groupage et de distribution des journaux périodiques énonce que « *la diffusion de la presse imprimée est libre* ». Ces textes pionniers ne discriminent aucun type de support de communication et les communications par voie de presse puis par la radio et la télévision sont irriguées par ce principe fondamental de libre communication. Depuis, la construction du système législatif consacrant cette liberté n'a cessé de progresser, de s'affirmer et de s'enrichir au fil des évolutions technologiques. La liberté de communication audiovisuelle est consacrée par la loi n° 82-652 du 29 juillet 1982 sur la communication audiovisuelle qui dispose que : « *la communication audiovisuelle est libre* » (art. 1er). Il n'existe dès lors aucune objection à ce que ce principe ait vocation à s'appliquer au nouveau support de communication qu'est l'internet. La loi n° 2000-719 du 1er août 2000 modifiant la loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication avait aligné les services de communication en ligne sur le même régime de liberté que celui applicable aux services de communication audiovisuelle (art. 1er al. 1er et art. 2). Dans son titre premier intitulé « *De la liberté de communication en ligne* », la loi du 21 juin 2004 pour la confiance dans l'économie numérique a affirmé : « *La communication au public par voie électronique est libre* » (art. 1er).

[327] *U.S. Const. amend.* I.

[328] V. *supra* : n° 150.

[329] Le juge BRANDEIS estime que si « *le droit à la liberté de parole, le droit d'enseigner et le droit de réunion sont, bien entendu, des droits fondamentaux* [...] *ils ne sont pas, dans leur nature, absolus* » (*Whitney v. California*, 274 *U.S.* 357, spéc. 373 (May 16,1927)). – V. également, Laurent PECH, *Liberté de communication en droit comparé*, fasc. préc., spéc. n° 38.

[330] Si le discours politique jouit d'une protection forte, le gouvernent peut imposer des restrictions raisonnables à cette forme d'expression, v. en ce sens Mark SWEET, " Political E-Mail : Protected Speech or Unwelcome Spam? ", 2003 *Duke L. & Tech. Rev*. 1 (2003), spéc. p. 3 (" *restrictions on the time, place, and manner* ").

[331] La mise en place de cet équilibre n'est pas sans rappeler le principe de proportionnalité existant dans le système européen (sur ce point, v. not. Laurent PECH, « Liberté de communication en droit comparé », fasc. préc., spéc. n° 40 et s.).

droit absolu [332]. L'examen de constitutionnalité portait sur une disposition légale permettant notamment à toute personne destinataire de courriers de demander au *Potsmaster General* de faire cesser des envois futurs à cette adresse et de la supprimer des listes de diffusion [333]. Les juges de première instance qui avaient reconnu la constitutionnalité de cette disposition [334], avaient provoqué le mécontentement d'éditeurs, distributeurs, entreprises de vente par correspondance, courtiers de listes de diffusion qui avaient fait appel de cette décision, plaidant l'inconstitutionnalité de cette disposition dans la mesure où elle affectait le développement de leur activité [335]. Il appartenait alors à la Cour Suprême de déterminer si la liberté de communication, indispensable dans une société démocratique, ne pouvait souffrir d'aucune restriction tel que le soutenaient les appelants [336]. En l'espèce, si la Cour reconnaissait cette liberté comme impérative dans un ordre social sain, toute personne devait bénéficier d'une autonomie suffisante lui permettant d'exercer un contrôle sur les courriers non sollicités [337]. Pour cela, il était essentiel que le destinataire en soit le seul et dernier juge [338]. À ce titre, la Cour Suprême relevait que le Congrès avait permis au citoyen « *d'ériger un mur* » que les annonceurs n'avaient pas le droit de franchir sans leur consentement [339]. C'est donc de façon catégorique que la Cour Suprême rejetait la défense des appelants. Après avoir jugé d'une part, que la liberté de communication ne devait en aucun cas porter atteinte à leur *right to be left alone* et d'autre part, que le « *droit de communiquer d'un annonceur* [devait] *s'arrêter à la boîte aux lettres d'un destinataire non réceptif* » [340], elle a ainsi conclu à la constitutionnalité de la réglementation gouvernementale qui limitait les envois commerciaux aux seuls destinataires qui le souhaitaient [341]. Cette décision est donc une application de la théorie américaine du « *balancing approach* » dont l'expression apparaît clairement dans la motivation du juge FRANKFURTER dans l'affaire *Bridges vs California* de 1941 [342]. Le pragmatisme de cette théorie exhortant à établir un juste équilibre entre la liberté d'expression et les autres intérêts en concurrence, interdit toute

[332] *Rowan v. United States Post Office Dept*., 397 *U.S*. 728, spéc. 728 (May 4, 1970).
[333] *Idem*, spéc. 728.
[334] *Id., loc. cit.*
[335] *Id.*, spéc. 729.
[336] *" The freedom to communicate orally and by the written word and, indeed, in every manner whatsoever, is imperative to a free and sane society* " (*id.*, spéc. 735).
[337] *Id.*, spéc. 736.
[338] *Id., loc. cit.*
[339] *" Congress* […] *permits a citizen to erect a wall that no advertiser may penetrate without his acquiescence "* (*id.*, spéc. 738).
[340] *"* [The] *mailer's right to communicate must stop at the mailbox of an unreceptive address "* (*Rowan*, aff. préc., spéc. 737). La Cour Suprême l'a confirmé par la suite : *" We therefore categorically reject the argument that a vendor has a right, under the Constitution or otherwise, to send unwanted material into the home of another.* […] *The asserted right of a mailer, we repeat, stops at the outer boundary of every person's domain "* (*id.*, spéc. 738).
[341] *Id.*, spéc. 740.
[342] *Bridges v. California*, 314 *U.S*. 252 (Dec. 8, 1941).

conception « *absolue et irrationnelle* » de la liberté d'expression qui risquerait d'entraver l'exercice d'autres droits proclamés dans le *Bill of Rights* [343].

B. LA LIBERTE D'EXPRESSION A L'EPREUVE DU *SPAMMING*

154. Pour légitimer l'exercice de leur activité, les « spammeurs » ont tenté de démontrer l'inconstitutionnalité tant des techniques de filtrage anti-*spam* utilisées par les FAI (1.) que celle des lois anti-*spam* (2.) au regard du Premier amendement. Afin de mesurer la pertinence de ces défenses et évaluer l'étendue de la protection constitutionnelle accordée à cette liberté en matière de *spamming*, deux affaires retiendront tout particulièrement notre attention.

1. La question de la constitutionnalité des techniques de filtrage

155. L'affaire *Cyber Promotions, Inc. v. America Online* [344]. En l'espèce, la société AMERICA ONLINE Inc. (ci-après, AOL) se plaignait de l'envoi par la société CYBER PROMOTIONS (ci-après, CYBER PROMOTIONS) de messages commerciaux non sollicités à ses abonnés. Confrontée à la réception de nombreuses plaintes de ces derniers et face à l'ignorance des demandes adressées à CYBER PROMOTIONS visant à cesser de tels envois, AOL avait décidé de filtrer et de collecter tous les *spams* provenant de cet expéditeur et de les retourner au FAI du « spammeur ». CYBER PROMOTIONS avait alors déposé une plainte sollicitant de la cour qu'elle lui accorde le droit de poursuivre son activité et qu'elle interdise à AOL de prendre toutes mesures destinées à bloquer la réception de ses *e-mails* [345]. Pour sa défense, CYBER PROMOTIONS prétendait que le recours à de telles techniques de filtrage violait son droit à la liberté d'expression. La *U.S. District Court for the Eastern District of Pennsylvania* avait relevé que le Premier amendement protégeait la liberté d'expression des citoyens américains contre les atteintes commises par le gouvernement mais non contre celles causées par les personnes privées [346]. Après avoir jugé qu'un FAI ne pouvait avoir ni la qualité d'acteur public ni celle de service public [347], la Cour en avait ainsi déduit que CYBER

[343] *Id.*, spéc. 282: " *Free speech is not absolute or irrational a conception as to imply paralysis of the means for effective protection of all the freedoms secured by the Bill of Rights* ".
[344] *CompuServe, Inc. v. Cyber Promotions, Inc.*, aff. préc. – *CompuServe, Inc. v. Cyber Promotions, Inc*., aff. préc.
[345] *Cyber Promotions*, 948 *F. Supp*. 436, aff. préc., spéc. 437.
[346] *Id.*, spéc. 441.
[347] Sur ces refus, v. *supra :* n° 150

PROMOTIONS ne pouvait valablement se fonder sur la protection du Premier amendement contre AOL. Cette affaire confirme donc clairement que les FAI ont le droit de limiter l'accès à leur serveur par l'utilisation de tous moyens légaux disponibles et peuvent notamment recourir à des mécanismes de blocage du nom de domaine de CYBER PROMOTIONS ou à tout autre dispositif de filtrage destiné à éviter que ses membres ne reçoivent des *spams* [348]. Cette solution doit être, selon nous, saluée puisqu'elle est l'expression d'un compromis entre les intérêts économiques et la liberté de choix des internautes à recevoir ou non des *e-mails* commerciaux.

2. La question de la constitutionnalité des lois anti-*spam*

156. Le test de constitutionnalité issu de l'affaire *Central Hudson* : un test en quatre étapes. L'examen de constitutionnalité d'un texte législatif au regard du Premier amendement relève d'un test particulier d'origine jurisprudentielle. Ce dernier a été développé dans l'affaire *Central Hudson* [349], considérée comme la décision de référence en la matière puisque la Cour Suprême fournit aux magistrats les lignes directrices décrivant la démarche à suivre pour vérifier la constitutionnalité des restrictions portées au discours commercial [350]. La Cour Suprême a ainsi défini quatre conditions qui, lorsqu'elles sont réunies, peuvent justifier qu'une atteinte soit portée à la liberté d'expression commerciale. La première consiste à vérifier que le discours commercial est protégé par le Premier amendement [351]. À cette fin, la Cour doit rechercher s'il concerne une activité licite qui n'est pas destinée à tromper les consommateurs [352]. Dans l'affirmative, l'examen se poursuit en s'assurant que le gouvernement [353] justifie d'un intérêt substantiel dans la réglementation du

[348] 948 *F. Supp*. 436, aff. préc., spéc. 456 (refusant au demandeur une injonction contre l'utilisation du logiciel de filtrage). – Dans le même sens, v. *CompuServe*, 962 *F. Supp*. 1015, aff. préc., spéc. 1019.
[349] *Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n of New York*, arrêt préc. Depuis cette décision la Cour a reconnu que le discours commercial jouissait d'une certaine protection sans toutefois que celle-ci soit aussi importante que celle accordée aux autres formes de discours (*id*, spéc. 563).
[350] Dans cette affaire, il s'agissait de vérifier la constitutionnalité de la réglementation proposée par le gouvernement et visant à limiter la liberté d'expression commerciale. – Sur cette affaire, v. not. Michael W. CARROL, " Garbage In : Emerging Media and Regulation of Unsolicited Commercial Solicitations ", 11 *Berkeley Tech. L.J.* 233, spéc. p. 238 (1996). – John MAGEE, " The Law Regulating Unsolicited Commercial E-Mail : an International Perspective ", 19 *Santa Clara Computer & high Tech. L. J.* 333, spéc. p. 358 et s. (2003). – Gary S. MOOREFIELD, Note, " *SPAM* – It's Not Just for Breakfast Anymore : Federal Legislation and the Fight to Free the Internet from Unsolicited Commercial E-mail ", 5 *B.U. J. Sci. & Tech. L.* 10, spéc. p. 3 et s. (1999). – Ian J. SILVERBRAND, " Commercialspeech.com : ACPA and the First Amendment ", art. préc., spéc. pp. 19-21. – Jan H. SAMORISKI, " Unsolicited Commercial E-mail, the Internet and the First Amendment : Another Free Speech Showdown in Cyberspace? ", 43 J. *Broad. & Elec. Media* 670, spéc. p.685 (1999).
[351] *Cent. Hudson Gas & Elec. Corp.*, aff. préc., spéc. 566.
[352] *Id*., spéc. 563-564, 566.
[353] Le gouvernement américain est divisé en trois branches : législative, exécutive et judiciaire. Le Congrès des États-Unis est le parlement bicaméral composé de la Chambres des Représentants et du Sénat. Le Congrès est

discours commercial, autrement dit, que la mesure gouvernementale revêt un caractère sérieux [354]. La preuve du caractère substantiel est subordonnée à la démonstration de la réalité des atteintes que la mesure envisagée a vocation à restreindre [355]. La troisième condition exige d'établir que la mesure en question sert directement cet intérêt gouvernemental [356]. L'objectif est d'évaluer la pertinence de la mesure en confrontant les intérêts étatiques à la restriction envisagée [357]. Enfin, le test se conclut en vérifiant le caractère proportionnel de la mesure au regard de l'objectif. À cette fin, il appartient aux magistrats de s'assurer que cette mesure n'apparaît pas plus étendue que nécessaire [358], étant précisé que le gouvernement n'est pas tenu de choisir les moyens les plus restrictifs possibles [359].

157. Application du test à la réglementation anti-*spam*. Dans la mesure où nous n'avons pas encore étudié la loi anti-*spam* fédérale américaine, le *CAN-SPAM Act*, nous concentrerons notre analyse sur certaines dispositions communes à la majorité des lois anti-*spam* des États en vigueur avant l'adoption de la législation fédérale, dispositions que nous retrouverons dans le *CAN-SPAM Act* à l'occasion d'une étude qui lui sera exclusivement consacrée [360].

158. Première étape : l'exigence de licéité du *spamming*. Cette condition exclut d'emblée de l'examen de constitutionnalité les *spams* qui visent à tromper les destinataires en déguisant les en-têtes des messages pour dissimuler l'origine véritable de l'expéditeur ou en insérant dans les messages – objet ou corps – des informations fausses destinées à inciter

chargé d'élaborer, de discuter et de voter les lois. Le terme « gouvernement » utilisé dans les prochains développements désigne la branche législative.

[354] *Id*., spéc. 566, 568-569.

[355] *Edenfield v. Fane*, 507 *U.S*. 761, spéc. 761-762 (Apr. 26, 1993).

[356] *Cent. Hudson Gas & Elec. Corp.*, aff. préc., spéc. 566, 569.

[357] *Id*., spéc. 569.

[358] *Id*., spéc. 566, 569-570.

[359] *Board of Trustees of State University of New York v. Fox*, 492 *U.S*. 469, spéc. 476-477 (June 29, 1989).

[360] Sur la confrontation de la législation anti-*spam* au Premier amendement, lire not. Michael W. CARROL, " Garbage In : Emerging Media and Regulation of Unsolicited Commercial Solicitations ", art. préc. – Michael A. FISHER, " The Right to Spam? Regulating Electronic Junk Mail ", 23 *Colum.- Vla J.L. & Arts* 363 (2000). – Alex KOZINSKI & Stuart BANNER, "Who's Afraid of Commercial Speech? ", 76 *Va. L. Rev*. 627 (1990). – John MAGEE, " The Law Regulating Unsolicited Commercial E-Mail: an International Perspective", 19 *Santa Clara Computer & High Tech L.J* 333 (2003). – J. A. MARCUS, " Commercial Speech on the Internet : *Spam* and the First Amendment ", 16 *Cardozo Arts & Ent. L.J*. 245 (1998). – Gary S. MOOREFIELD, " *SPAM* – It's Not Just for Breakfast Anymore : Federal Legislation and the Fight to Free the Internet from Unsolicited Commercial E-mail ", art. préc. – Jan H. SAMORISKI, " Unsolicited Commercial E-mail, the Internet and the First Amendment : Another Free Speech Showdown in Cyberspace? ", art. préc. – Pour une analyse détaillée de la constitutionnalité du *CAN-SPAM Act*, v. not. Marc SIMON, Note, " The CAN-SPAM Act of 2003 : Is Congressional Regulation of Unsolicited Commercial E-Mail Constitutional? ", 4 *J. High Tech. L.* 85 (2004). – Pour une application de ce test au *Telephone Consumer Protection Act* de 1991 (TPCA) et plus précisément à la disposition 47 *U.S.C.* Sec. 227(b) (1) (C) qui interdit l'envoi de publicité non sollicitée par télécopie, et jugée constitutionnelle au regard du Premier amendement, v. not. *Missouri ex rel. Nixon v. American Blast Fax, Inc.*, 196 *F. Supp.2d* 920 (E.D. Mo. 2002), *rev'd*, 323 *F.3d* 649 **(**8th Cir. 2003). – *Destination Ventures, Ltd. v. Federal Communications Commission*, 46 *F.3d* 54, spéc. 55 (9th Cir. Feb. 1, 1995).

les destinataires à les ouvrir [361]. En dehors de ces cas de figure, le *spamming* est considéré comme licite et est dès lors susceptible de recevoir la protection du Premier amendement. On bascule alors vers la deuxième étape du test qui consiste à vérifier si le gouvernement justifie d'un intérêt substantiel dans l'adoption de cette réglementation anti-*spam.*

159. Deuxième étape : la preuve d'un intérêt substantiel. Eu égard à la nature perturbatrice du *spamming* et aux coûts élevés qu'il peut engendrer pour les « spammés », il semble aisé de considérer cette pratique comme un problème assez sérieux pour admettre que le gouvernement ait un intérêt substantiel à l'adoption de mesures anti-*spam.* Rappelons en effet que l'envoi de *spams* est incroyablement bon marché et permet au « spammeur » d'expédier des centaines de milliers de messages dans un laps de temps très court et à un coût dérisoire puisque ce dernier est répercuté sur les destinataires. Par ailleurs, l'afflux massif de *spams* engendre le plus souvent de lourdes dépenses pour les FAI, contraints notamment de financer l'achat de bande passante supplémentaire afin d'éviter que leurs serveurs ne soient perturbés, voire paralysés. Enfin, la réception d'un flot important de *spams* peut entraîner une perte de temps substantielle pour lire, trier et supprimer les messages indésirables au risque de perdre, d'ignorer ou de mettre au rebus des courriers légitimes [362]. L'intervention du gouvernement est donc justifiée d'une part, par le souci de diminuer les conséquences financières que subissent les « spammés » et d'autre part, par la volonté d'assurer la viabilité et l'utilité des services de l'internet et notamment des messageries électroniques [363].

160. Troisième étape : la pertinence de la mesure. Pour passer le filtre constitutionnel, la mesure envisagée doit promouvoir directement un intérêt gouvernemental et s'appliquer dans les limites des objectifs poursuivis. Afin d'illustrer comment s'opère le contrôle de cette exigence, nous raisonnerons à partir de deux des dispositions majeures présentes dans la plupart des lois des États et que l'on retrouvera dans le *CAN-SPAM Act* [364]. La première concerne l'obligation de respecter les demandes de désinscription (demandes d'*opt-out*). Selon cette disposition, tout destinataire de *spams* a le droit de s'opposer à l'envoi futur de *spams*, l'objectif poursuivi étant de diminuer le volume de *spams* reçus. La seconde,

[361] Ce type de messages ne pourra recevoir la protection du Premier amendement et sera alors régi par la loi anti-*spam* sans que cette dernière ne subisse l'examen de constitutionnalité.
[362] Sur l'ensemble des conséquences dommageables causées par le *spamming*, v. *supra* : n° 44 et s.
[363] Michael A. FISHER, " The Right to Spam? Regulating Electronic Junk Mail ", art. préc., spéc. p. 409 (" [t]*he governmental interest in preserving the viability of e-mail as a medium of communication is likely to be considered substantial if there is a real danger that this medium will be rendered useless without regulation* " (Trad. Libre : « l'intérêt gouvernemental dans la préservation de la viabilité du courrier électronique comme moyen de communication va probablement être considéré comme substantiel s'il existe un réel danger que ce moyen soit rendu inutile sans réglementation »)).
[364] V. *infra* : n° 323 et s.

relative à l'obligation de mentionner une adresse de retour valide, est destinée à rendre efficace le droit d'opposition puisqu'elle permet au destinataire de soumettre sa demande à l'expéditeur ainsi identifié. Au regard de la finalité de ces obligations, celles-ci peuvent, sans difficultés, être considérées comme justifiées pour répondre à l'un des objectifs visé par le gouvernement, à savoir la préservation de la viabilité du service de messagerie électronique.

161. Quatrième étape : le caractère proportionné de la mesure. Pour mémoire, il s'agit ici de vérifier que la réglementation porte le mois possible atteinte à la liberté d'expression commerciale. À cet égard, une décision mérite d'être citée car elle permet de mieux saisir les contours de cette exigence : l'affaire *Jeremy Jaynes* dans laquelle a été déclarée inconstitutionnelle la loi anti-*spam* de Virginie au motif qu'elle était plus étendue que nécessaire. On se souviendra de l'une des premières condamnations prononcées sur le fondement de la loi anti-*spam* de Virginie [365] dont l'exemplarité avait été remarquée, tant par le volume des *spams* émis que par la sanction prononcée en novembre 2004 [366]. Une recherche au domicile de Jeremy JAYNES, surnommé le « Roi du spam », avait révélé l'existence d'une base de données titanesque puisqu'elle contenait cent soixante seize millions d'adresses électroniques complètes et un milliard trois cent mille adresses électroniques partielles [367]. Il était reproché à ce dernier d'avoir envoyé pas moins de dix millions de *spams* par jour, dont plus de 55.000 sur une période de dix jours à des abonnés d'AOL [368]. Par ailleurs, pour masquer son identité, Jeremy JAYNES avait falsifié certaines informations identifiantes avant de distribuer les messages [369] *via* de multiples adresses [370]. Malgré ses efforts pour rester anonyme, il avait néanmoins été identifié comme l'expéditeur de la plupart des *e-mails* [371]. Reconnu coupable pour l'envoi massif de *spams* en violation de la loi anti-*spam* de Virginie, ce dernier avait été condamné en première instance à neuf ans de prison [372], condamnation confirmée par la cour d'appel de Virginie en 2006 [373]. Cette dernière avait rejeté les arguments de Jeremy JAYNES qui avait tenté de dénoncer l'inconstitutionnalité de la loi anti-*spam* de Californie, sur le fondement de laquelle il avait

[365] La loi interdit la transmission de courrier électronique non sollicité dans le cas où le contrevenant (1) utilise un ordinateur avec l'intention de falsifier les informations de transmission et (2) le courrier électronique passe par le réseau informatique d'un prestataire de services. Le délit devient un crime (*felony*) si, comme dans le cas de Jeremy JAYNES, le nombre d'envois s'il dépasse 10.000 messages en vingt-quatre heures ou 100.000 en un mois ou un million en un an, et sanctionné d'une peine de prison (*Va. Code Ann*. § 18.2-152.3:1 (2008)).
[366] *Jeremy Jaynes v. Commonwealth of Virginia*, 666 *S.E.2d* 303, 276 *Va*. 443 spéc. 450 (2008).
[367] *Id.*, spéc. 449.
[368] *Id.*, spéc. 448.
[369] *Id.*, spéc. 449 (" [Jaynes] *intentionally falsified the header information and sender domain names before transmitting the e-mails to the recipients* "). – V. ég. *id.*, note 3.
[370] *Id.*, spéc. 450.
[371] *Id.*, spéc. 449 (" [*I*]*nvestigators used a sophisticated database search to identify JAYNES as the sender of the e-mails* ").
[372] *Id.*, spéc. 450.
[373] *Jeremy Jaynes v. Commonwealth of Virginia*, 48 *Va. App*. 673 (2006).

été reconnu coupable, au regard du Premier amendement. Pour sa défense, il reprochait à cette loi son champ d'application trop large et soutenait qu'elle violait son droit à s'exprimer anonymement, protégé par le Premier amendement [374]. Confirmant les décisions des juges du fond, la Cour suprême de Virginie avait jugé, par une décision rendue le 3 mars 2008 et adoptée par 4 voix contre 3, que la liberté d'expression garantie par le Premier amendement de la Constitution américaine interdisait le *spamming* [375]. Toutefois, à la suite de la demande de révision sollicitée par Jeremy JAYNES, la Cour suprême a adopté une position renversant complètement sa propre décision adoptée six mois auparavant [376]. La Cour reprochait à cette loi son champ d'application trop large en constatant que l'interdiction concernait tout envoi d'e-*mails* non sollicités, massifs et anonymes, quel que soit leur contenu (politique, religieux ou autre) [377]. La loi anti-*spam* de Virginie était donc unique en ce qu'elle visait potentiellement à criminaliser la transmission de tout type de courrier électronique massif non sollicité, sans se limiter aux *e-mails* à caractère commercial ou aux discours frauduleux, diffamatoires ou obscènes non protégés par la Constitution américaine [378]. La Cour Suprême a dès lors déclaré l'inconstitutionnalité de cette loi anti-*spam* au motif qu'elle violait le droit au discours anonyme protégé par le Premier amendement et que la falsification des informations portant sur l'identification de l'émetteur d'un courrier électronique constituait le seul moyen permettant à ce dernier de masquer efficacement son identité et d'exercer son droit de s'exprimer de façon anonyme [379]. À travers cette décision, les juges américains ont démontré que si la liberté d'expression commerciale pouvait être limitée selon des critères strictement définis, cette restriction ne devait pas compromettre l'exercice de la liberté d'expression dans son ensemble. Au-delà de son apport quant au champ d'application de la liberté d'expression et les incidences qu'elle peut avoir sur la législation anti-*spam*, cette décision laisse clairement transparaître toutes les difficultés qui naissent autour de la restriction du champ des lois anti-*spam* au caractère exclusivement commercial du contenu

[374] *Id*, spéc. 453-459. – L'argumentaire de Jeremy Jaynes reposait sur la doctrine du « *overbreadth* », doctrine selon laquelle une loi dont la rédaction est trop large viole implicitement la liberté d'expression protégée par le Premier amendement. – Pour une étude générale sur la protection du discours anonyme par le Premier amendement, v. Miguel E. LARIOS, " E-Publius Unum: Anonymous Speech Rights Online ", 37 *Rutgers Law Record* 36 (2010).

[375] *Id.* spéc. 443, note 2.

[376] *Id.* spéc. 448, 450, note 5, *cert. denied*, 129 *S. Ct.* 1670 (2009).

[377] *Id*. spéc. 463-464.

[378] Contrairement à la loi de Virginie, la loi *anti-spam* fédérale américaine, le *CAN-SPAM Act Act* (108th Congress, Pub. L. n° 108-187, 117 Stat. 2699 (2003). – Sur cette loi, v. *infra* : n° 323)), limite cette prohibition aux seuls messages qui ont vocation à promouvoir une activité commerciale, en excluant tous ceux à but non lucratif. – *Jeremy Jaynes*, *id*., spéc. 461 (« *Many other states have regulated unsolicited bulk e-mail but, unlike Virginia, have restricted such regulation to commercial e-mails* »).

[379] *Id.* spéc. 461 (" *By prohibiting false routing information in the dissemination of e-mails, CODE § 18.2-152.3:1 infringes on that protected right* ") ; *Id.* spéc. 464 (finding that the statute is " *unconstitutionally overbroad on its face because it prohibits the anonymous transmission of all unsolicited bulk e-mails including … speech protected by the First Amendment to the United States Constitution* ").

du message [380]. En effet, la liberté d'expression et dans ce cas particulier, le droit au discours anonyme ne peut connaître aucune restriction dès lors qu'il entre dans le champ du discours protégé (discours politique ou religieux). Aussi, est-il à craindre, que cette situation ne génère des comportements abusifs permettant à certains individus mal attentionnés, sous couvert de leur droit à la liberté d'expression, de « bombarder » anonymement les messageries électroniques d'*e-mails* non commerciaux.

*****

*** * ***

162. De façon générale, il ressort de l'ensemble de ces affaires que la défense des « spammeurs » fondée sur la liberté d'expression ait peu de chance de triompher. En effet, malgré une protection forte de cette liberté aux États-Unis, elle n'est pas totale et connaît certaines limites en matière commerciale qui ne semblent pas plaider en faveur des « spammeurs » américains. Si cet argument d'ordre économique apparaît comme une justification faible au soutien du *spamming*¸ la valeur économique potentielle des données nominatives semble être une motivation suffisamment forte pour poursuivre leur activité et intensifier la collecte d'adresses électroniques, en raison notamment des gains importants qu'ils peuvent retirer de cette activité. Il en résulte que si l'évolution des données nominatives vers une logique marchande n'est ni condamnable ni dangereuse en elle-même, elle devient source croissante d'inquiétudes dès lors qu'elle est porteuse de menaces pour les données à caractère personnel et qu'elle favorise le développement du *spamming* qui nuit au bon fonctionnement des services de messageries.

[380] Sur le champ d'application des lois anti-*spam :* v. *infra* : n° 296 et s.

SECTION II. UNE INQUIÉTUDE SOCIALE CROISSANTE

163. Source de richesses informationnelles et financières, les adresses électroniques éveillent chez les « spammeurs » un vif désir d'appropriation à des fins d'exploitation commerciale. L'accroissement des captations furtives et des manipulations opaques, favorisé par des moyens techniques de collecte très variés [381], engendre un risque d'utilisation et de réutilisation des données insoupçonné parce que généralement insoupçonnable. Face à ces manipulations de plus en plus expertes, le contrôle des titulaires sur leurs données paraît dès fortement s'affaiblir à tel point que celui-ci semble totalement leur échapper (§ 1.). Cette crainte grandissante face au risque d'exploitation abusive des données est d'autant plus perceptible et justifiée qu'une fois les adresses électroniques collectées, les titulaires éprouvent les plus grandes difficultés à lutter contre le déferlement de *spams* et à faire respecter leur droit à être laissé tranquille (§ 2.).

§ 1. LA PERTE DE CONTROLE DES TITULAIRES SUR LEURS DONNEES

164. La dématérialisation et la volatilité des données nominatives ont décuplé les possibilités de les capter et les enregistrer à des fins de traitements massifs. En effet, cette identité numérique, morcelée et aisément accessible (A.), accentue l'opportunité de les exploiter, notamment à des fins publicitaires, mais les expose également à un risque croissant de dérives qui justifie la revendication d'un droit à la protection des données par leurs titulaires (B.).

A. UNE IDENTITE NUMERIQUE AISEMENT ACCESSIBLE, SOURCE DE DERIVES

165. Une identité parcellée exposée à de multiples captations. Dans le cyberespace, l'internaute n'apparaît plus comme une entité unique, immuable mais se compose d'une multitude de représentations numériques, se déclinant sous la forme d'adresses électroniques, de logs, de mots de passe, etc. et qui seront communiquées à l'occasion des divers actes effectués sur l'internet : *e-mails* échangés, participations à des forums de discussions ou à des sites communautaires, acquisition de biens ou souscription à des services. Les passages répétés de chaque internaute sur le réseau laissent inéluctablement

[381] V. *supra* : n° 91 et s.

de multiples traces qui rendent la navigation sur l'internet tout sauf anonyme [382]. En effet, contrairement à une idée que beaucoup se plaisent à croire, l'ensemble de ces actes réalisés sur l'internet est loin d'être anodin : le choix de cliquer sur tel lien hypertexte ou d'ouvrir telle fenêtre publicitaire ou encore de remplir un formulaire d'inscription en ligne constitue autant d'opportunités de captation des données nominatives, le plus souvent à l'insu de leur titulaire [383]. Comme le souligne le professeur Jean FRAYSSINET, « [a]*vec les nouvelles technologies le consommateur joue le Petit Poucet : sans toujours en avoir conscience, il laisse derrière lui des petits cailloux blancs que des tiers ramassent pour les utiliser parfois contre ses intérêts… Un consommateur nu sous le regard des tiers n'est plus un consommateur libre !* » [384]. La CNIL, il y a plus de dix ans, exprimait déjà son inquiétude face à la « *mémoire d'internet* » devenant le « *monde des traces invisibles qui défient les principes de la protection des données* » [385]. Aussi, le mythe de l'anonymat incarné par le célèbre adage « O*n the Internet, nobody knows you're a dog* » apparaît-il définitivement suranné [386].

166. Les dérives inhérentes à la captation de l'identité numérique. Comme nous avons pu le voir précédemment lorsque nous avons expliqué comment les « spammeurs » procédaient à la collecte de données [387], la circulation des données sur le réseau leur permet de les capter très facilement afin de construire ou d'alimenter de vastes bases de données dans lesquelles elles seront engrangées sans que les internautes en aient conscience. Il suffira par la suite aux « spammeurs » de puiser dans ces stocks de données pour procéder à des envois massifs, sans risquer d'éveiller le moindre soupçon de la part des futurs destinataires, si ce n'est à l'arrivée de *spams* sur les messageries. Ces risques de captation et d'exploitation totalement opaques ne cessent de s'accroître en raison des moyens de plus en plus

[382] À cet égard, le professeur Jean FRAYSSINET explique que « *les traces sont consubstantielles à l'usage des NTIC et des services offerts pour des raisons techniques (l'acheminement de l'information vers le demandeur par exemple) et économiques (identification du demandeur pour le paiement du service rendu)* » (« La traçabilité des personnes sur l'internet », art. préc., spéc. pp. 76.-77 ; « La traçabilité des personnes sur l'internet, une possible menace pour les droits et libertés », art. préc., (*in* Philippe PEDROT (sous la dir.), *Traçabilité et responsabilité*, Economica, 2003) spéc. pp. 90-91). Et « *Internet*, [en particulier] *ne peut fonctionner sans gérer des traces* » (*id.*, spéc. p. 78). – V. ég. CNIL, « Internet sans trace, ça n'existe pas ! », actualités, 11 janv. 2010, disponible sur : http://www.cnil.fr/la-cnil/actu-cnil/article/article/internet-sans-trace-ca-nexiste-pas/ ; Dossier CNIL, « Vos traces sur internet : ce n'est pas virtuel ! », disponible sur : http://www.cnil.fr/vos-libertes/vos-traces/.

[383] Michel DUPUIS, « La Vie privée à l'épreuve de l'internet : quelques aspects nouveaux », art. préc. – Jean FRAYSSINET, « La traçabilité des personnes sur l'internet », art. préc., spéc. p. 81 et s.

[384] Jean FRAYSSINET, « Nouvelles technologies de l'information et de la communication et protection des libertés des consommateurs », art. préc., spéc. p. 42.

[385] CNIL, *Rapport d'activité 1996*, rapport préc., spéc., p. 67.

[386] Littéralement : « *Sur l'Internet, personne ne sait que tu es un chien* ». Cet adage trouve son origine dans une caricature de Peter Steiner parue dans le New Yorker qui parodie l'anonymat existant sur l'internet en représentant un chien installé à un bureau devant un ordinateur et s'adresse à un autre chien en lui prononçant les paroles pré-citées. (*New* Yorker, 5 juillet 1993, vol. 69, (LXIX), n° 20, p. 61). Pour visualiser cette illustration, consulter l'adresse suivante : http://www.unc.edu/depts/jomc/academics/dri/idog.html.

[387] V. *supra :* n° 91 et s.

performants permettant de tracer les internautes [388]. Les publicitaires font feu de tous bois pour atteindre leurs objectifs. Tous les média et mode de communication sont exploités : télévision, radio, panneaux d'affichage, tracts, … C'est donc sans surprise que l'internet a été rapidement utilisé à des fins publicitaires [389] puisqu'il permet aux annonceurs de développer leur activité promotionnelle à moindre coût par rapport aux médias traditionnel, selon un mode interactif où les internautes sont incités à cliquer sur des liens hypertextes pour collecter de nouvelles informations. Surtout, il permet de proposer une offre de plus en plus personnalisée [390] grâce notamment au recours aux fameux *cookies*, ces petits fichiers textes enregistrés sur le disque dur de l'ordinateur de l'internaute à la demande du serveur du site Internet consulté. Cette traçabilité n'est pas mauvaise en elle-même et les *cookies* constituent une bonne illustration des aspects positifs que peut revêtir la traçabilité. Ils permettent en effet aux internautes de faciliter leur navigation sur le réseau en conservant en mémoire les sites déjà consultés. En revanche, ce qui est beaucoup plus inquiétant c'est que cette traçabilité de l'internaute est devenue de plus en plus insidieuse et insoupçonnée grâce à des procédés très performants rendant ainsi illusoire toute tentative de se cacher derrière une identité virtuelle [391]. Le programme de publicité en ligne mis en place par GOOGLE, « *Ad by Google* » illustre cette opacité des opérations de traçabilité. À cet égard, le Comité consultatif de la Convention pour la protection des données à l'égard du traitement automatisé des données à caractère personnel attire l'attention sur le fait que « [c]*e que beaucoup de consommateurs ignorent c'est que les liens commerciaux apparaissant dans cette fenêtre sont générés au cas par cas et en temps réel par GOOGLE sur la base de la page référante communiquée par leur navigateur. GOOGLE peut donc suivre, pas à pas, la navigation de chaque internaute sur chacune des pages des sites à grande fréquentation (eBay, journaux en ligne, moteurs de recherches, sites boursiers, sites de vente immobilière, etc.)* » [392]. On peut encore citer l'outil de mesure et de trafic d'audience d'un site Internet, *Google Analytics*, qui permet notamment aux annonceurs de connaître, de façon relativement précise, la navigation des internautes grâce à la possibilité d'identifier le nombre de visites

[388] Les services de l'internet permettent en effet à quiconque d'indexer le nom d'une personne sur un moteur de recherche pour obtenir en quelques secondes toutes les données mises en ligne le concernant. À cet égard, Jean FRAYSSINET explique qu'« [à] *travers les nouvelles technologies, le consommateur-client se transforme en un ensemble informationnel qui donne lieu, unilatéralement ou bilatéralement, à collecte, stockage, traitement, transmission, diffusion de données par rapport aux fournisseurs de biens et de services* » (« Nouvelles technologies de l'information et de la communication et protection des libertés des consommateurs », art. préc., spéc. p. 33).

[389] V. par ex. Jean-Marc COBLENCE, « Publicité sur le net », *Expertises* 1997, p. 259 et s.

[390] V. *supra* : n° 147.

[391] « *Aujourd'hui, le simple fait d'allumer un ordinateur branché sur Internet met en route plusieurs processeurs qui exécutent subrepticement des centaines de programmes sans que l'utilisateur moyen en soit informé ni puisse avoir le moindre contrôle sérieux sur les données qui y sont traitées* ». Pour une vision complète des traitements invisibles : Jean-Marc DINANT, « Les traitements invisibles sur Internet », Les Cahiers du CRID n° 16, 1999, p. 277-302.

[392] Jean-Marc DINANT, Christophe LAZARO, Yves POUILLET, et al., *L'application de la Convention 108 au mécanisme de profilage*, rapport préc., spéc. p. 4.

par page d'un site *Web*, de calculer le pourcentage de visites au cours desquelles l'internaute a quitté un site dès la première entrée, de relever le nombre de fois qu'un internaute a cliqué sur une annonce, de comptabiliser le nombre d'entrées sur un même site, le nombre de nouvelles visites d'internautes accédant pour la première fois au site, d'identifier le nombre de sorties d'un site, d'indiquer le temps qu'un visiteur a passé sur une page ou un ensemble de pages, le nombre total de pages vues sur un site en tenant compte du critère sélectionné … Il permet également de renseigner sur le contenu des pages consultées : le nombre total d'utilisations de la fonction « Recherche » du site consulté, le nombre total de visites au cours desquelles le moteur de recherche interne au site a été utilisé, le temps passé sur un site, depuis la première recherche interne jusqu'à la fin de la session ou jusqu'au lancement d'une autre recherche… Les capacités de cet outil sont très puissantes puisqu'il permet également de calculer le nombre total d'articles vendus pour le produit (ou le groupe de produits), la valeur moyenne par visite correspond à la valeur moyenne d'une visite sur un site, le revenu par clic, la valeur moyenne d'une transaction en ligne, le nombre total de transactions [393].

167. Les nouveaux réseaux sans fil de faible portée. La popularité croissante des réseaux sans fil à faible portée tels que notamment ceux de type WIFI ou *Bluetooth* augmentent les risques pour les données à caractère personnel puisqu'ils permettent de suivre la trace de tout terminal équipé d'une interface WIFI ou *Bluetooth*, « *à l'insu de son détenteur et ce, même dans l'hypothèse où l'équipement terminal n'est pas volontairement activé* » [394]. À ce titre, Jean-Marc DINANT, docteur en informatique, directeur au Centre de Recherche Informatique et Droit (CRID) et expert judicaire, attire l'attention sur le fait que ces réseaux représentent aujourd'hui « *une menace majeure et insuffisamment prise en compte par rapport à la traçabilité des utilisateurs* » [395]. Il souligne à ce titre l'absence de confidentialité, faute de chiffrage systématique de ces réseaux. En particulier, par le biais du réseau WIFI, il est aisé pour un tiers de consulter le trafic entre un terminal sans fil et la borne WIFI. Et même dans le cas où ces réseaux seraient chiffrés, le numéro de série statique d'une

[393] Sur ces différentes fonctionnalités de *Google Analytics*, consulter la page disponible sur : http://www.google.com/support/analytics/bin/answer.py?hl=fr&answer=99118. – V. ég. un autre exemple de traçabilité, CNIL, « Dispositif d'analyse du comportement des consommateurs : souriez, vous êtes filmés ! », 19 avr. 2010, disponible sur : http://www.cnil.fr/la-cnil/actu-cnil/article/article/dispositifs-danalyse-du-comportement-des-consommateurs-souriez-vous-etes-comptes-2/ (à propos de dispositifs utilisant des téléphones portables pour mesurer la fréquentation de certains lieux ou des images vidéo afin de mesurer l'audience publicitaire).

[394] Jean-Marc DINANT, *Rapport sur les lacunes de la Convention n°108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel face aux développements technologiques (Partie I)*, rapport préc., spéc. p. 3.

[395] Jean-Marc DINANT, *Rapport sur les lacunes de la Convention n°108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel face aux développements technologiques (Partie I)*, rapport préc., spéc. p. 3.

borne WIFI ou un mobile *Bluetooth* est généralement lisible en clair. En effet, techniquement la borne ou le mobile répondent automatiquement à une tentative de connexion, même si elle est abusive et non suivie d'effet en communiquant leur numéro de série électronique unique au monde (*Global Unique Identifier*). Dans ces circonstances, toute personne connectée au réseau WIFI ou *Bluetooth* peut connaître un numéro de série *Bluetooth* ou l'adresse MAC d'une carte WIFI, sans même amorcer une véritable communication [396].

168. À travers ces quelques exemples on mesure combien les données nominatives sont exposées à des risques de captation et d'exploitation totalement occultes et dont les consommateurs ignorent la finalité de leurs utilisation. C'est précisément l'ignorance de ces derniers quant au devenir de leurs traces qui favorise l'accroissement de telles manipulations à leur insu [397] puisque les internautes apparaissent impuissants à anticiper un danger dont ils ne peuvent pressentir l'existence en amont.

B. LA REVENDICATION D'UN DROIT A LA PROTECTION DES DONNEES

169. La tentation du droit de propriété : Une tentative de protection avortée. La numérisation des informations a favorisé l'intensification des traitements de données et des collectes indiscernables [398]. Face aux abus pressentis, le législateur a été conduit à adopter la loi informatique, fichiers et libertés afin de protéger les individus contre la création de fichiers qui portent atteinte aux libertés individuelles. Toutefois, les nouveaux enjeux attachés à la marchandisation des données à caractère personnel et leur exploitation à des fins commerciales, favorisés par des moyens techniques permettant un traçage de plus en plus précis des individus [399] ne font qu'accroître les dangers qui pèsent sur les données. Afin de protéger ces dernières un peu plus efficacement, les fervents défenseurs d'un droit de

[396] Jean-Marc DINANT, *Rapport sur les lacunes de la Convention n°108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel face aux développements technologiques (Partie I)*, rapport préc. spéc. p. 3.

[397] Ce constat est particulièrement frappant à la lecture des conclusions formulées, à propos des moteurs de recherche, par le Groupe « article 29 » lequel observe que « *la plupart des utilisateurs internet n'ont pas conscience de la quantité significative des données relatives aux comportements lors des recherches qui font l'objet d'un traitement et des finalités de ce traitement* » (G29, Avis n° 1/2008 sur les aspects de la protection des données liés aux moteurs de recherche, 00737/FR,WP 148, 4 avril 2008, spéc. p. 22, disponible sur : http://www.cnil.fr/fileadmin/documents/approfondir/dossier/internet/wp148_fr.pdf). – La conclusion est identique pour les utilisateurs de sites communautaires, v. en ce sens : Winston J. MAXWELL, Thomas ZEGGANE et Sarah JACQUIER, « Publicité ciblée et protection du consommateur en France, en Europe et aux États-Unis », *Cont. conc. conso.* juin 2008, Étude 8, p. 18 et s.

[398] « *La crainte de voir l'homme s'emparer totalement de l'homme est devenue le cœur de toutes les angoisses* » (Monique CONTAMINE-RAYNAUD, *Le secret de la vie privée, in* Yvon LOUSSOUARN et Paul LAGARDE (sous la dir.), *L'information en droit privé. Travaux de la conférence d'agrégation*, L.G.D.J., coll. *Bibl. dr. privé*, 1978, p. 402 et s., spéc. n° 36, p. 454).

[399] V. *supra* n[os] : 166-167.

rétention en faveur des titulaires ont alors plaidé en faveur de la reconnaissance d'un droit de propriété sur les données nominatives [400]. Si cette thèse semble de prime abord séduisante, elle est, d'un point de vue éthique, extrêmement dangereuse et remet en cause le rapport de l'homme à lui-même [401]. En tant qu'attribut de la personnalité [402], le nom patronymique, par exemple, a pour fonction d'identifier la personne individuellement [403] et de lui conférer une appartenance au sein d'un groupe : la famille et plus largement, la société. Intimement lié à son titulaire, ce dernier ne peut en être privé. Le nom patronymique, et plus largement les attributs de la personnalité, sont hors du commerce, inaliénables, imprescriptibles et opposables à tous [404]. Leur extra-commercialité des attributs de la personnalité interdit que ces derniers fassent l'objet de conventions [405].

170. Le rapport entre le titulaire et ses données défini comme un droit de la personnalité. Si le rapport de droit entre l'individu et les données le concernant ne peut s'analyser en un droit réel, ni même en un droit personnel, c'est-à-dire un droit sur autrui, c'est parce qu'on est, « *avec l'information personnelle, dans un rapport à sa propre*

[400] V. not. Pierre CATALA, « Ébauche d'une théorie juridique de l'information », *D.* 1984, chron. p. 97 et s. (« *La législation de protection des données reconnaît aux individus des prérogatives considérables sur les données qui les concernent nommément, les droits d'accès et de rectification en particulier. La même loi ouvre aux personnes la faculté de s'opposer, pour des raisons légitimes, à leur inclusion dans un fichier nominatif ; elle leur donne, enfin, le droit d'exiger des renseignements de celui qui recueille l'information* […]. *Ce sont là des prérogatives du droit réel. Elles consacrent implicitement l'appartenance de la donnée nominative à la personne concernée, légitime titulaire qui peut, en cette qualité, vérifier leur bon usage et leur véracité* »).

[401] Nathalie MALLET-POUJOL, « Appropriation de l'information : l'éternelle chimère », chron. préc., spéc. n° 20, p. 334 (« *Imaginer des prérogatives de propriétaires sur ses propres données est, du point de vue éthique, inconcevable dans la mesure où l'individu ne dispose pas de lui-même, pas plus qu'il ne vend ses informations* »). – Frédéric, LESAULNIER, *L'information nominative*, thèse préc., spéc. n° 322, p. 286 (« *Si la personne devient propriétaire de ses attributs, ils ne peuvent plus lui être identifiés mais deviennent des objets de droit " ordinaires ". L'appropriation des informations personnalisées consacrera le passage de la chose au bien, donc leur déshumanisation complète, au prix de ce qui en fait l'unité de la personne. À la maîtrise de la personne pourra se substituer, par cession ou concession, la maitrise de la personne d'autrui. Qui ne voit pas que c'est tout le rapport de l'homme à lui-même qui est en cause dans ce pouvoir de s'aliéner soi-même à autrui* »).

[402] Corinne FILIPPONE explique que certains attributs remplissent « *une fonction de différenciation en les distinguant les uns des autres par leur nom, leur image et leur voix* ». Permettant ainsi d'identifier les titulaires, ils sont dits « *endogènes* », alors que d'autres, comme la vie privée, sont dits « *exogènes* » car ils « *ne contribuent pas à la désignation de leur titulaire* » et « *ne se rattachent à la personne qu'en raison de l'exercice d'une activité quelconque* » (*La contractualisation des droits de la personnalité*, thèse de doctorat en droit, sous la direction de Philippe DELEBECQUE, Paris I, 2001, spéc. n° 5, p. 13). – V. ég. Laure MARINO, « Les contrats portant sur l'image des personnes », *Comm. com. électr.* mars 2003, chron. 7, p. 10 et s. (l'image permet l'identification de la personne et est inséparable de cette dernière : elle « *lui est inhérente, intrinsèque ; elle fusionne avec elle, et elle va évoluer aussi avec elle, elle va vieillir avec elle* »).

[403] Selon le professeur Grégoire LOISEAU, « *il est de coutume d'analyser le nom comme un attribut de la personnalité et l'associe ainsi, dans l'esprit des tiers, à celui qui désigne* » (*Le nom objet d'un contrat* (préf. Jacques GHESTIN), tome 274, L.G.D.J., coll. *Bibl. dr. privé*, 1997, spéc. n^{os} 373, p. 369).

[404] V. François CHABAS et Florence LAROCHE-GISSEROT, *Les personnes – La personnalité – Les incapacités*, tome 1, vol. 2, 6^{e} éd., Montchrétien, coll. *Leçons de droit civil Henri, Jean et Léon MAZEAUD*, 1997, spéc. n° 565, p. 617.

[405] Nathalie MALLET-POUJOL, « Appropriation de l'information : l'éternelle chimère », chron. préc., spéc. n° 20, p. 334.

personne » [406]. Le droit de l'individu sur ces données à caractère personnel est un droit de la personnalité, une « *prérogative de l'homme* » [407]. Les droits de la personnalité sont « [l]*es droits de la personne humaine qui appartiennent de droit à tout personne physique pour la protection de ses intérêts primordiaux* » [408] Le professeur Loïc CADIET rappelle que « *les droits de la personnalité sont nés de l'impossibilité d'analyser les rapports de la personne avec les attributs qui lui sont propres comme des droits de la personnalité* » [409]. Constituent notamment des droit de la personnalité le droit au respect de la vie privée, le droit au nom protégeant l'individu contre toute usurpation ou l'utilisation non autorisée de son patronyme par autrui, le droit à l'image, droit de s'opposer à la reproduction de son image par des tiers non autorisés. Ces droits connaissent toutefois certains tempéraments, justifiés par les intérêts des tiers, notamment leur droit à l'information. En effet, si l'information nominative permet à chaque individu d'exister et de s'affirmer à travers ses particularités, sa personnalité, il est en même temps un maillon de la chaîne sociale [410]. La circulation des informations est dès lors inhérente à la vie sociale [411.] L'individu doit être envisagé dans une sphère collective où le droit de contrôle revendiqué par leur titulaire sur leurs données est limité par un droit reconnu aux tiers d'y avoir accès. Dans cette perspective, il s'agit dès lors d'abandonner toute approche qui consisterait à multiplier les obstacles à la vocation première de l'information, c'est-à-dire sa circulation, et à son exploitation pour s'attacher à construire un cadre juridique de protection des données destiné à empêcher les abus et les excès de certains traitements. Le droit doit ainsi s'attacher à trouver un compromis entre ces intérêts concurrents. La délicate articulation entre ces derniers impose de structurer les rapports de façon à préserver la qualité des prérogatives reconnues à chacun [412]. Si le titulaire ne dispose

[406] Nathalie MALLET-POUJOL, « Appropriation de l'information : l'éternelle chimère », chron. préc., spéc. n° 21, p. 334. – Laure MARINO, « Les contrats portant sur l'image des personnes », *Comm. com. électr.* mars 2003, chron. 7, p. 10 et s. (l'image permet l'identification de la personne et est inséparable de cette dernière : elle « *lui est inhérente, intrinsèque ; elle fusionne avec elle, et elle va évoluer aussi avec elle, elle va vieillir avec elle* »).

[407] Nathalie MALLET-POUJOL, « Appropriation de l'information : l'éternelle chimère », chron. préc., spéc. n° 21, p. 334.

[408] Gérard CORNU, Vocabulaire Juridique, *op. cit., loc. cit.*

[409] Loïc CADIET, « La notion d'information génétique en droit français », *in* Bartha Maria KNOPPERS et Claude M. LABERGE, *La Génétique humaine, de l'information à l'informatisation,* éd. Litec/Thémis, 1992, p. 41 et s., spéc. p. 60.

[410] « *une personne est non seulement un être physique et psychique mais aussi un être informationnel* » (André LUCAS, Jean DEVEZE et Jean FRAYSSINET, *Droit de l'informatique et de l'Internet,*). – Yves POULLET, « Le fondement du droit de la protection des données nominatives : " Propriété ou Libertés ", *in* Ejan MACKAAY, *Nouvelles Technologies et propriété : actes du colloque tenu à la faculté de droit de l'Université de Montréal,* les 9 et 10 novembre 1989, Thémis, Montréal, 1991, p. 175 et s. (« *L'information, même nominative, est une représentation de la réalité sociale, qui ne peut être la propriété exclusive de l'individu auquel est rattachée cette donnée. L'individu est plongé dans une société, un environnement social, il représente une forme d'électron lié et inclus dans un ensemble plus vaste qu'est la société* »).

[411] « *il n'y a pas de vie sociale sans échanges de données personnelles* » (André LUCAS, Jean DEVEZE et Jean FRAYSSINET, *Droit de l'informatique et de l'Internet*, P.U.F., coll. *Thémis Droit privé*, Paris, 2001, spéc. n° 10, p. 9).

[412] Le professeur Nathalie MALLET-POUJOL souligne que « *la grande caractéristique des conventions d'exploitation d'informations personnelles est la mention de restrictions dans l'usage des données. Ces clauses protègent la personne contre les contractants ou contre elle-même et participent de l'approche personnaliste du droit* ». Ces montages contractuels « *ne sont pas justifiés par un rapport de propriété qui entraverait toute*

pas de ses données nominatives, il doit bénéficier des prérogatives lui permettant d'en exploiter l'usage et donc de pouvoir en interdire ou en limiter l'usage par autrui [413], et empêcher ainsi les excès et les abus de certains traitements. La loi informatique, fichiers et libertés illustre cet objectif d'équilibre qu'il convient d'atteindre et participe à la reconnaissance de ces droits de la personnalité. L'article premier rappelle que « [l'informatique] *ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques* ». Le lien qui unit les données à leurs titulaires leur confère certains droits sur leurs données qui tracent ainsi les limites dans lesquelles doivent se développer les traitements informatiques en veillant toutefois à ne pas les paralyser. Il apparaît dès lors que cet équilibre autour duquel se forge le rapport qui unit la donnée à son titulaire doit être trouvé [414] et se caractériser par la fixation de droits et d'obligations permettant l'exercice d'un droit de jouissance par son titulaire mais également par la société.

171. La reconnaissance au titulaire de données d'un droit d'en exploiter l'usage. Si les titulaires ne peuvent disposer de leurs informations personnelles, ils conservent toutefois le droit d'en exploiter l'usage et d'en contrôler l'utilisation par des tiers, ces données n'étant « *ni de libre parcours, ni de libre usage* » [415]. En effet, comme le souligne le professeur Nathalie MALLET-POUJOL, « [i]*l paraîtrait insolite de nier la possibilité pour l'individu d'exploiter l'usage des informations le concernant quand on constate l'importance de la pratique contractuelle et l'empirisme dans la construction d'un tel droit* » [416]. Pour le comprendre, nous prendrons l'exemple du nom patronymique et de

utilisation de données personnelles par des tiers, mais prennent en compte les droits de l'individu sur ses données tout en recherchant l'équilibre entre intérêts et libertés en présence, au regard notamment du caractère privé ou sensible des informations en cause » (« Appropriation de l'information : l'éternelle chimère », chron. préc., spéc. n° 29, p. 336).

[413] Selon Nathalie MALLET-POUJOL, « Appropriation de l'information : l'éternelle chimère », chron. préc., spéc. pp. 333-335).

[414] Le risque de surveillance n'est pas en soi le problème majeur, ce qui le devient est l'utilisation inadéquate des données à caractère personnel et le détournement de finalités pour lesquelles ces données étaient initialement destinées. À cet égard, la CNIL rappelle que l'important pour la personne concernée par ses données est *« d'avoir la garantie que ces données ne seront pas détournées de la finalité initiale, communiquées à des tiers qui n'ont pas à en connaître* » (CNIL, *Rapport d'activité 2001*, n° 22, Doc. fr., 2002, spéc. p.108).

[415] Frédéric LESAULNIER, *L'information nominative*, Thèse sous la dir. de Pierre CATALA, Paris II, 2005, spéc. n° 97, p. 129.

[416] Nathalie MALLET-POUJOL, « Appropriation de l'information : l'éternelle chimère », chron. préc., spéc. n° 24, p. 335. – V. ég. Grégoire LOISEAU, *Le nom objet d'un contrat, ibid.*, spéc. p. 167 et s. –Michel VIVANT, « Le patronyme saisi par le patrimoine », art. préc., p. 517, spéc. n° 8 et s., p. 521 et s. – Sur l'existence de clause de prix et de cession du droit d'utiliser un nom patronymique (v. par ex. Frédéric POLLAUD-DULIAN, note sous TGI Paris, 17 sept. 2004, RG n° 02/15485, *Inès de la Fressange*, *JCP* 2004, éd. G., II. 10182). – Sur l'existence du contrat d'image, v. CA Versailles, 12e ch., 2e sect., 22 sept. 2005, *Sas Calendriers Jean Lavigne*, arrêt préc. (« *dès lors que le droit à l'image revêt les caractéristiques essentielles des attributs d'ordre patrimonial, il peut valablement donner lieu à l'établissement de contrats, soumis au régime général du droit des obligations, entre le cédant, lequel dispose de la maîtrise juridique sur son image, et le cessionnaire lequel devient titulaire des prérogatives attachées à ce droit* ». – Cass. civ. 1re, 24 oct. 2006, pourvoi n° 04-17.560, *Sté VF Films Production et Sté Nationale de télévision France 3 c/ X*, *Juris-Data* n° 2006-035517 ; *Legipresse* déc. 2006, I, p. 172 et

l'image dont la valeur économique est devenue incontestable. Si dans sa fonction d'identification, cet attribut de la personnalité conserve son caractère indisponible, il acquiert toutefois une certaine autonomie lui permettant de se détacher de son titulaire et devenir disponible [417]. Faisant œuvre de pragmatisme à cet égard, la jurisprudence française a en effet su dépasser la conception personnaliste traditionnelle pour admettre que le principe d'inaliénabilité ne constituait plus un obstacle insurmontable à l'exploitation commerciale du nom patronymique à titre de signe distinctif, comme la marque, le nom commercial ou la dénomination sociale [418]. Corollaire du détachement entre l'attribut et son sujet, « *le patronyme joue ainsi un rôle de personnalisation des produits et constitue certainement un facteur de proximité en associant, aux yeux des acheteurs potentiels, le produit à celui qui le fabrique* » [419]. En devenant un moyen de promouvoir des produits ou services, le nom peut à ce titre représenter une source de profits. Tel est le cas du fondateur d'une société qui autorise sa société, personne morale, à utiliser son nom patronymique comme signe distinctif [420]. De même, l'exploitation commerciale de la renommée confirme cette pratique si l'on pense aux hypothèses, devenues fréquentes, où un sportif de haut niveau [421], un acteur de cinéma, un mannequin ou un commerçant reconnu dans son secteur d'activité autorise la commercialisation de son nom notoirement connu à des fins de promotion d'un produit ou d'un service [422]. Ce mouvement de patrimonialisation n'est pas exclusif au nom

Legipresse janv.-févr. 2077, III, p. 1, note L. Marino (reconnaissant la validité des contrats d'image à condition qu'ils ne portent pas atteinte au respect de l'image de la personne ni à sa vie privée).

[417] En ce sens, v. Michel VIVANT, « Le patronyme saisi par le patrimoine », *in Mélanges André Colomer*, Litec, Paris, 1993, p. 517 et s., spéc. n° 5, p. 519 (« *le nom peut devenir une valeur patrimoniale, objet marchand* […] *en acquérant une autonomie par rapport à son titulaire* »).

[418] Cass. com. 12 mars 1985, *Bordas*, pourvoi n° 84-17.163 ; *Rev. sociétés* 1985, p. 607, note G. Parleani ; *D.* 1985. jurispr., p. 471, note J. Ghestin ; *JCP* 1985, éd. G., II. 20400, concl. M. Montanier et note G. Bonet ; *Gaz. Pal*. 1985, 1, p. 246, note G. Le Tallec (« *le principe de l'inaliénabilité du nom patronymique* […] *ne s'oppose pas à la conclusion d'un accord portant sur l'utilisation de ce nom comme dénomination sociale ou nom commercial* […] *ce patronyme est devenu, en raison de son insertion* […] *dans les statuts de la société* […], *un signe distinctif qui s'est détaché de la personne physique qui le porte pour s'appliquer à la personne morale qu'il distingue et devenir ainsi objet de propriété incorporelle* »). – Dans le même sens, Cass. com., 27 févr. 1990, *Mazenod*, pourvoi n° 88-19.194 *; JCP* 1990, éd. G., II. 21545, note F. Pollaud-Dulian. – Cass. com. 13 juin 1995, *Petrossian*, *Dr. sociétés* 1996, comm. 51, obs. Th. Bonneau. – Même solution dans l'hypothèse d'un nom patronymique notoire, v. not. en ce sens Cass. com. 6 mai 2003, *Ducasse*, pourvoi n° 00-18.192, *Juris-Data* n° 2003-018973, *D.* 2003, jurispr., p. 2228, note G. Loiseau ; *Comm. com. électr*. juill.-août 2003, comm. 70, note C. Caron*; JCP* 2003, éd. G., II. 10169, note E. Tricoire ; *RTD civ*. 2003, p. 679, obs. J. Hauser. – Cass. com. 24 juin 2008, *Beau*, pourvois n[os] 07-10.756 et 07-12.115, *Bull. Joly* 2008, p. 953, note G. Loiseau ; *D.* 2008. 2569, note A. Mendoza-Caminade; *JCP* 2008, éd. E., 2466, note C.-A. Maetz; *Rev. Sociétés* 2009, p. 587, note G. Parléani ; *Droit* des *sociétés* 2009, comm. 23, note M.-L. Coquelet ; *Comm. com. électr*. déc. 2008, comm. 133, p. 31 et s., note C. Caron.

[419] Grégoire LOISEAU, *Le nom objet d'un contrat, op. cit.*, spéc. n° 172, p. 181.

[420] V. not. Théo HASSLER, « La crise d'identité des droits de la personnalité », *LPA* 7 déc. 2004, n° 244, p. 3 et s. – Grégoire LOISEAU, *Le nom objet d'un contrat, op. cit.*, spéc. n[os] 170-181, pp.180-189. – Éric LOQUIN, « L'approche juridique de la marchandisation », *in* Éric LOQUIN et Annie MARTIN (sous la dir.), *Droit et marchandisation*, Litec, Paris, 2010, p. 79 et s., spéc. n[os] 36-37, p. 93.

[421] V. par ex. Éric LOQUIN, « L'approche juridique de la marchandisation », art. préc., spéc. n[os] 44-52, pp. 97-100. – Gérald SIMON, « La marchandisation du sportif : l'opération de transfert du footballeur », *in* Éric LOQUIN et Annie MARTIN (sous la dir.), *Droit et marchandisation, op. cit.*, p. 305 et s.

[422] CA Toulouse, 15 avr. 2003, *M. Barthez c/ Sté Hachette Filipacchi Associés*, *inédit*. – Cass. com. 6 mai 2003, *Ducasse*, arrêt préc. – CA Aix-en-Provence, 2[e] ch., 25 nov. 2004, *D.* 2005, p. 845 et s., note Didier Poracchia et

patronymique et s'est étendu à d'autres attributs de la personnalité tels que l'image des personnes ; la jurisprudence [423] comme la doctrine [424] ont reconnu l'existence d'un détachement entre l'image et la personne concernée [425]. Cette valorisation économique du nom patronymique a ainsi conduit une partie de la doctrine à reconnaître la nature dualiste du droit au nom : à l'instar de la dichotomie existant en droit d'auteur, certains auteurs défendent l'idée selon laquelle il existerait un droit de la personnalité originel qui n'est nullement remis en cause auquel viendrait se greffer un droit patrimonial distinct lorsque le titulaire cède ou concède le droit d'exploiter commercialement son nom [426]. On retrouve également cette nature dualiste pour le droit à l'image [427]. Cette conception tend de ce fait à

Claude-Albéric Maetz (à propos de l'insertion dans une dénomination sociale d'un nom patronymique connu et le dépôt de ce même nom à titre de marque).

[423] Selon les juridictions du fond, l'existence d'un droit patrimonial à l'image est manifeste dès lors que celle-ci fait l'objet d'une exploitation commerciale procurant des profits (v. en ce sens, TGI Lyon, 17 déc. 1980, *Asvel Basket et Gilles et a. c/ Sté Anon et Lumière et Sté Anon-Euro-Advertising*, *D.* 1981, jurispr., p. 202, note R. Lindon et D. Amson. – TGI Marseille, 6 juin 1984, *Izzo c/ Sté Seppim* (2e espèce), *D.* 1985, somm., p. 323 et s., obs. R. Lindon (« *la personne est lésée dans son droit patrimonial sur son image, dès lors que, sans son consentement, il en est fait une exploitation commerciale, le préjudice résultant de ce qu'elle n'a pas été associée au profit ainsi réalisé* »). – CA Paris, 2 février 1993, *Melle Baillie et autres*, *D.* 1993, I.R., p. 118 (à propos de l'image d'un mannequin). – TGI Paris, 3e ch., 2e sect., 28 sept. 2006, *E. Thomas et 2 Secondes production c/ Réservoir Prod.*, *Legipresse* 2006, I, p. 160 et s. et *ibid.* 2007, II, p. 18 et s., obs. Th. Hass ; *Ibid.* mars 2007, III, p. 54 et s., note J.-M. Bruguière. – CA Versailles, 12e ch., 2e sect., 22 sept. 2005, *SAS Calendriers Jean Lavigne c/ Sté Universal Music*, *Juris-Data* n° 2005-288693; *Comm. com. électr.* janv. 2006, comm. 4, p. 29 et s., note C. Caron ; *Legipresse* 2006, III, p. 109, comm. J.-M. Bruguière ; *D.* 2006, p. 2705, obs. L. Marino (l'artiste « *concède au licencié un droit exclusif de reproduire de quelque manière que ce soit* […] *son image* »).

[424] Jean-Michel BRUGUIERE, note sous TGI Paris, 28 sept. 2006, *Evelyne THOMAS et 2 Secondes Production*, jugement préc., *Légipresse* mars 2007, n° 239, p. 54 et s.). – V. ég. Jean-Michel BRUGUIERE et Bérangère GLEIZE, obs. sous Cass. civ. 1re, 25 janv. 2000, pourvoi n° 97-15.163, *X c/ Sté Presse Alliance et a.* ; *Juris-Data* n° 2000-000257. – Selon les termes du professeur Christophe CARON, « *un nouveau droit voisin est né : le droit patrimonial sur l'image* » (note sous CA Versailles, 22 sept. 2005, *SAS Calendriers Jean Lavigne c/ Sté Universal Music et al.*, arrêt préc., *Com. comm. électr*. janv. 2006, comm. 4, p. 29 et s.). – V. ég. Emmanuel GAILLARD, « La double nature du droit à l'image », *D.* 1984, chron., p. 161 et s. – Grégoire LOISEAU , note sous Cass. civ. 1re, 13 janv. 1998, *D. c/ Sté Jag.*, *JCP* 1998, éd. *G*., II. 10082. – Éric LOQUIN, « L'approche juridique de la marchandisation », art. préc., spéc. nos 38, p. 93. – Marie SERNA, « L'image et le contrat : le contrat d'image », *Cont. conc. conso*. nov. 1998, chron. 12, p. 4 et s. (l'image est « *reproductible à l'infini* » (*id.*, spéc. n° 3, p. 4) et permet ainsi de prouver le détachement entre cette dernière et la personne qu'elle singularise). – Sur la possible admission d'un droit patrimonial sur l'intimité de la vie privée, v. Éric LOQUIN, « L'approche juridique de la marchandisation », art. préc., spéc. nos 39, p. 94 (prenant l'exemple des contrats conclus à titre onéreux par des personnalités assurant à certains groupes de presse l'exclusivité de la révélation d'informations, de photos ou encore de films portant sur leur vie privée).

[425] Cette distanciation entre la donnée nominative et son titulaire est encore plus exacerbée s'agissant des identifiants numériques. À ce titre, l'adresse IP en est l'exemple le plus manifeste puisque celle-ci n'identifie que le réseau local de l'ordinateur connecté. L'adresse électronique illustre également ce détachement. En effet, même si elle contient le plus souvent le nom, voire le prénom de son titulaire, elle n'identifie pas directement son titulaire mais seulement sa messagerie électronique.

[426] Sur l'ambivalence du nom patronymique, v. Grégoire LOISEAU, *Le nom objet d'un contrat*, *ibid.*, spéc. n° 373, p. 369. – Emmanuel TRICOIRE, note sous Cass. com., 6 mai 2003, arrêt préc., *JCP* 2003, éd. G., II. 10169. –Selon Frédéric POLLAUD-DULIAN, « *la jurisprudence Bordas-Mazenod incite à s'interroger à nouveau sur la nature du droit sur le nom patronymique, puisque, semblant bien repousser l'idée d'un droit exclusivement personnel, elle conduit à se demander s'il ne s'agit pas d'un droit dualiste* » (note sous Cass. com. 27 févr. 1990, *Mazenod*, arrêt préc., *JCP* 1990, éd. G., II. 21545).

[427] V. en ce sens, TGI Aix-en-Provence, 1re ch., 24 nov. 1988, *Brun c/ SA Expobat et a.*, *JCP* 1989, éd. G., II. 21329, obs. J. Henderycksen (« *le droit à l'image a un caractère moral et patrimonial* »). – Comp. Cass. civ. 1re, 11 déc. 2008, n° 07-19.494, F P+B, *Brossard-Martinez c/ Sté Photoalto*, *JCP* 2009, éd. G., II. 10025, G. Loiseau (la Cour de cassation ne tranche pas clairement la question. – Le professeur Grégoire LOISEAU, regrettant la position timide de la Cour de cassation, exhorte à cesser « *de camoufler les choses : il est grand temps de reconnaître ouvertement, franchement, officiellement, la réalité du droit patrimonial à l'image* » (note sous

importer dans notre droit la *suma divisio* d'origine américaine qui oppose le *right of privacy*, non évaluable en argent au *right of publicity* qui, au contraire, est évaluable et monnayable. Cette reconnaissance par la doctrine et la jurisprudence doit être saluée car l'adoption d'une position inverse aurait eu pour conséquence de compromettre l'avenir des conventions permettant au titulaire d'un nom ou d'une image d'en exploiter l'usage alors même que leur existence constitue un impératif pratique incontestable et surtout parce qu'une fois ces données introduites dans la sphère marchande, le rapport de droit qui unit la donnée à son titulaire perdure. La reconnaissance d'une valeur économique aux données à caractère personnel ne conduit nullement à mettre la personne dans le commerce. En effet, comme l'explique le professeur Grégoire LOISEAU, « *la patrimonialité n'est pas celle du nom envisagé comme représentation de la personne mais n'affecte en réalité ce signe que comme support incident de la notoriété du sujet.* […] *il en résulte que cette patrimonialité ne conduit pas dès lors à mettre un prix sur la personne humaine mais témoigne plutôt de la valeur de la notoriété qui peut être conçue, quant à elle, comme un véritable bien patrimonial* » [428].

Cass. civ. 1re, 11 déc. 2008, arrêt préc. *JCP* 2009, éd. G., II. 10025). – V. aussi Christophe CARON, note sous CA Versailles, 12e ch., 2e sect., 22 sept. 2005, note préc. (« *à l'instar du droit d'auteur, le droit à l'image a dorénavant une nature dualiste : aux côtés d'un droit moral à l'image, il existe un droit patrimonial sur l'image* »). – V. ég. Emmanuel GAILLARD, « La double nature du droit à l'image », chron. préc., spéc. p. 161 (le droit patrimonial à l'image « *se traduirait par la reconnaissance d'un monopole à chaque individu sur la réalisation et la diffusion de sa propre image valant dispense de prouver autre chose que l'atteinte portée à ce monopole pour en obtenir la sanction en justice* »). – Nathalie MALLET-POUJOL, « Appropriation de l'information : l'éternelle chimère », chron. préc., spéc. n° 24, p. 335 (« *accepter une possible exploitation de l'image ne signifie pas abandonner la théorie personnaliste. L'individu dispose, sur son image, de certaines prérogatives patrimoniales mais qui ne sauraient remettre en cause la qualification de droit de la personnalité. Nous souscrivons ainsi à une théorie que l'on pourrait qualifier de " dualiste-personnaliste "* »). – Frédéric POLLAUD-DULIAN, « Droit moral et droits de la personnalité », *JCP* 1994, éd. G., I. 3780. – *Contra* Muriel FABRE-MAGNAN, « Propriété, patrimoine et lien social », *RTD civ.* 1997, p. 583 et s.

[428] Grégoire LOISEAU, *Le nom objet d'un contrat, op. cit.*, spéc. n° 375, p. 371. – V. ég. Éric LOQUIN, « L'approche juridique de la marchandisation », art. préc., spéc. n° 45, p. 97 (à propos de la marchandisation du sportif de haut niveau, précise que si le football apparaît comme « *le plus marchandisé des sports* », « [i]*l ne s'agit pas* […] *d'un marché portant sur la personne des sportifs, mais d'un marché portant sur la force de travail de ces derniers* »). – Toujours dans ce domaine du football, le professeur Gérald SIMON affirme clairement que la pratique fréquente des conventions de transfert « *ne constitue pas une vente d'être humain* ». « *La personne n'est pas directement l'objet de la prestation promise* » (« La marchandisation du sportif : l'opération de transfert du footballeur », art. préc., p. 318). – À propos de l'image, v. par ex. Laure MARINO, « Les contrats portant sur l'image des personnes », chron. préc., spéc. p. 11 (pour qui, l'objet du contrat d'image est nécessairement extérieur à l'image de la personne dans la mesure où l'image ne se détache pas de la personne : même fixée sur un support, celle-ci ne se distingue pas de la personne. Elle soutient ainsi que ce n'est ni l'image en tant que telle ni la notoriété de la personne qui intéressent l'exploitant mais « *le crédit de considération* » lequel « *serait une valeur patrimoniale transmise dans le contrat* ». Selon elle, le contrat d'image « *s'analyse comme l'engagement de ne pas exercer son droit de défense vis-à-vis de son cocontractant pendant un certain temps* […]. Cette *renonciation ne porte pas du tout sur le droit à l'image lui-même*, […] *mais précisément sur l'exercice du droit à l'image. La patrimonialisation s'explique ainsi : c'est le prix de la renonciation (temporaire) à agir en justice* »).

§ 2. LA REVENDICATION D'UN DROIT A ETRE LAISSE TRANQUILLE

172. La nécessité d'une reconnaissance par le droit des diverses formes de harcèlement informationnel. Les nouvelles technologies (téléphone mobile, messagerie électronique, télécopie, etc.) exposent les consommateurs, et plus largement les utilisateurs de ces modes de communication, à la réception très régulière, voire quasi quotidienne de messages non sollicités. Comme nous l'avons vu précédemment, des « pondeuses d'appels » permettent de générer une multitude d'appels de façon simultanée. En matière de *spamming*, des logiciels spécifiques permettent d'expédier simultanément une multitude de messages. Cette exposition des consommateurs à la réception envahissante suscite la gêne, voire l'exaspération. Pour l'hypothèse précise qui intéresse notre étude, à savoir la relation entre un « spammé » et un « spammeur », cette gêne pourra également être ressentie dans les cas où ce « spammé » est la cible de multiples envois simultanés de la part d'un même « spammeur » (*mail bombing*). Comme le souligne le professeur Jean FRAYSSINET, [i]*l s'agit d'une véritable forme de harcèlement informationnel qui porte atteinte à une certaine conception de la liberté du consommateur* » [429]. En droit américain, le droit à être laissé tranquille est consacré depuis longtemps [430] dans le cadre du droit de la *privacy* [431]. En France, la violation de ce droit à été poursuivie et sanctionnée dans des affaires de harcèlement téléphonique sur le fondement de l'article 222-16 du Code pénal qui punit d'un an d'emprisonnement et de 15.000 euros d'amende « *les appels téléphoniques malveillants réitérés ou les agressions sonores en vue de troubler la tranquillité d'autrui* » [432]. Une autre

[429] Jean FRAYSSINET, « Nouvelles technologies de l'information et de la communication et protection des libertés des consommateurs », art. préc., spéc. p. 42.

[430] Cette notion a fait l'objet d'une première étude aux États-Unis en 1890 : Samuel D. WARREN et Louis D. BRANDEIS, " The Right to Privacy ", *Harv. L. Rev.* 193 (1890). – V. ég. Sabah S. AL-FEDAGHI, " The " Right to be left alone " and Private Information " *in* Chin-Sheng CHEN, Joaquim FILIPE et al., *Enterprise Information Systems VII*, Springer, 2006, p. 157 et s. ; "The Right of Privacy" *in* Roy L. MOORE and Michael D. MURRAY, *Media Law and Ethics*, Routledge, 3rd ed., 2007, 816 p., spéc. p. 517 s., spéc. p. 527: " The Black's Law Dictionary defines right of privacy as "*the right to be let alone ; the right of a person to be free from unwarranted publicity* ".

[431] *Holloman v. Life Ins. Co of Virginia*, 7 S.E.2d 169 (1940) (« *The right to privacy is correctly defined* […] *as the right to be left alone ; the right of a person to be free from unwarranted publicity* »). – V. Jacques VELU, *Le droit au respect de la vie privée : Conférences données à la faculté de droit de Namur, Chaire René Cassin*, (préf. René CASSIN), Presses Universitaires de Namur, coll. *Travaux de la Faculté de droit de Namur*, Namur et Bruxelles, 1974, spéc. n° 19, pp. 20-21. – Sur le concept de *privacy*, v. David KORZENIK, « La protection des droits de la personnalité aux États-Unis et en Grande-Bretagne : aspects de droit comparé », *in Les nouvelles frontières de la vie privée, Legicom* n° 43, 2009/2, p. 51 et s., spéc. p. 53 (« *la privacy n'est pas un concept unique, mais un mot pour plusieurs intérêts différents* », qui se décompose en quatre catégories d'infractions, à savoir « *l'intrusion, la divulgation de faits publics, la présentation d'une personne sous un jour défavorable ou trompeur et l'appropriation du nom ou de l'image d'une personne à des fins commerciales* »).

[432] V. en ce sens, la Cour de cassation a considéré que le délit d'appels téléphoniques malveillants étaient constitués, que les appels « *soient reçus directement ou sur une boîte vocale* » (Cass. crim. 20 févr. 2002, *Bull. civ.* 2002, n° 37 ; *D.* 2003, somm., p. 248, obs. S. Mirabail. – V. ég. CA Pau, 1re ch. corr., 14 avr. 2004, *Juris-Data* n° 2004-240039 ; *Jcp 2004, éd. G., IV.2995* (s'est rendu coupable du délit d'appels téléphoniques malveillants réitérés le prévenu qui avait appelé son ancienne amie près de trois cents fois en deux mois, appels parfois enregistrés sur le répondeur de la victime). – La Cour de cassation n'hésite pas à étendre la notion d'appels téléphoniques aux SMS (Cass. crim. 30 sept. 2009, pourvoi n° 09-80.373 ; *Juris-Data* n° 2009-049991 ;

disposition du Code pénal récemment crée incrimine également cette forme d'atteinte à la tranquillité. La loi d'orientation et de programmation pour la performance de la sécurité intérieure du 14 mars 2011 [433] a en effet inséré, dans le Code pénal, l'article 226-4-1 qui dispose que : « *Le fait d'usurper l'identité d'un tiers ou de faire usage d'une ou plusieurs données de toute nature permettant de l'identifier en vue de troubler sa tranquillité ou celle d'autrui, ou de porter atteinte à son honneur ou à sa considération, est puni d'un an d'emprisonnement et de 15.000 € d'amende. Cette infraction est punie des mêmes peines lorsqu'elle est commise sur un réseau de communication au public en ligne* ». Cette prise en compte progressive par le droit des diverses atteintes au droit être laissé tranquille doit être saluée. Elle reste néanmoins insuffisante et gagnerait à être étendue à d'autres comportements qui portent tout autant atteinte à ce droit et au premier rang desquels on peut citer le *spamming*.

173. L'autonomie du droit à la tranquillité et consécration officielle. Pour le moment, en l'absence d'autres textes consacrant ce droit, il est considéré comme une composante du droit à la vie privée : « *le respect de la vie privée se traduit essentiellement par un devoir d'abstention : laissez-moi tranquille* » [434]. Ce lien entre ces deux droits est expressément établi par la directive du 12 juillet 2002 qui interdit le *spamming* au motif qu'« *il importe de protéger les abonnés contre toute violation de leur vie privée par des communications non sollicitées* » [435]. La CNIL souligne pour sa part, qu'« [u]ne *composante majeure du respect de la vie privée s'affirme* […] *au travers d'un droit à la tranquillité, énoncé par plusieurs directives européennes et décliné par le droit français, tant pour le fax que pour le publipostage électronique non sollicité ou Spam* » [436]. Si ce droit est un prolongement du droit à la vie privée [437], il ne peut se satisfaire d'une assimilation plus ou

Bull. crim. n° 162, *Comm. com. électr.* déc. 2009, comm. 115, note A. Lepage (jugeant que « *la réception d'un SMS se manifeste par l'émission d'un signal sonore par le téléphone portable de son destinataire* »). – V. ég. CA Reims, ch. appels corr., 20 août 2008, RG n : 08/00579, *Juris-Data* : 2008-008914 (envoi de trente messages écrits sur le téléphone portable de la victime).

[433] Loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure du 14 mars 2011, J.O. du 15 mars 2011, p. 4582 et s.

[434] Jean CARBONNIER, Droit civil : *Les personnes*, tome 1, P.U.F., coll. *Thémis droit privé*, 2000, n° 87, p. 156.

[435] Considérant 40 dir. 2002/58/CE du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques, dite « Vie privée et communications électroniques ».

[436] CNIL, « Le droit d'être laissé tranquille », *in Rapport d'activité 2003*, n° 24, Doc. fr., 2004, spéc. pp. 57-73, spéc. p. 58, disponible sur : http://www.cnil.fr/en-savoir-plus/rapports-dactivite/. – De même en jurisprudence cette confusion a été faite où la cour d'appel de Bordeaux avait condamné une société au versement de dommages et intérêts à une personne destinataire d'une loterie publicitaire, en raison notamment de l'atteinte qu'elle constitue à la vie privée des personnes sollicitées alors qu'elles ne souhaitent que la tranquillité » (CA Bordeaux, 2 mars 1989, *SA France Direct Service c/ de Visme* : *INC Hebdo*, n° 635, 21 avr. 1989, p. 11 *in* Agathe LEPAGE, *Libertés et droits fondamentaux à l'épreuve de l'internet : Droits de l'internaute, liberté d'expression sur l'internet, responsabilité*, Litec, 2002, spéc. p. 55). .

[437] Jean FRAYSSINET, « Nouvelles technologies de l'information et de la communication et protection des libertés des consommateurs », art. préc., spéc. p. 42.

moins approchante du droit à la vie privée. Cette autonomie peut notamment s'illustrer à travers différentes utilisations abusives de l'adresse électronique d'un tiers à l'origine d'atteintes distinctes. D'une part, cette donnée peut être destinée à accéder à la messagerie de cette personne afin de prendre connaissance du contenu des *e-mails* adressés à cette dernière. Toute intrusion non autorisée dans la boîte électronique d'un tiers constituera alors une violation de la correspondance privée et, par extension, une atteinte au droit à la vie privée [438]. D'autre part, l'adresse électronique collectée par le « spammeur » à l'insu de son titulaire peut être utilisée à des fins d'envois de *spams.* Dans ce cas de figure, l'exploitation de l'adresse d'un tiers n'a pas vocation à pénétrer dans la vie privée d'un individu mais à permettre que le courrier électronique atteigne le destinataire visé. À travers ces exemples, il en résulte que toute atteinte à la tranquillité ne génère pas automatiquement une atteinte à la vie privée. L'impossibilité d'assurer la protection des « spammés » par le truchement du droit à la vie privée plaide en faveur de la reconnaissance d'un droit à la tranquillité autonome, rejoignant ainsi les vœux de certains auteurs [439]. Une consécration formelle de ce droit aurait ainsi pour bénéfice de préciser à la fois sa signification et sa fonction propre permettant aux intéressés de s'en prévaloir lorsqu'ils sont victimes d'une atteinte à ce droit.

*****

*** * ***

174. La numérisation des données nominatives favorise la collecte intensive de données destinées à de multiples traitements dont les titulaires ignorent la plupart du temps leur existence et laissent craindre des risques de dérives. La valorisation économique des données nominatives accentue les dangers pressentis au regard des multiples recoupements possibles entre ces données à des fins de marketing notamment. À ces menaces pesant directement sur les données à caractère personnel, se greffe la menace découlant de leur exploitation et qui permet d'inonder les messageries et de porter atteinte au droit à la tranquillité des titulaires de ces messageries. Ainsi, la construction d'un système juridique

[438] Art. 9 C. civ. : *« toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance »*. – V. toutefois, Agathe LEPAGE, *Libertés et droits fondamentaux à l'épreuve de l'internet, op. cit.*, spéc. p. 35 et s. (soulignant l'assimilation excessive de la violation des correspondances privées à celle de la vie privée).

[439] V. ég. V. Jean FRAYSSINET, « Nouvelles technologies de l'information et de la communication et protection des libertés des consommateurs », art. préc., spéc., p. 46. – Jean FRAYSSINET, Michel VIVANT, C. LE STANC, Lamy Droit de l'informatique et des réseaux, 2002, n° 2677 (favorables à la reconnaissance de ce droit à la tranquillité pour lutter contre des pratiques telles que le *spamming*, les *cookies* ou les *pop-ups*). – Kassem HALA, *L'internaute et son droit à être laissé tranquille*, Mémoire DEA, Montpellier, 2003. *Contra* : Agathe LEPAGE, *Libertés et droits fondamentaux à l'épreuve de l'internet, op. cit.*, spéc. pp. 55-56.

protecteur doit-elle s'inscrire dans une logique de gestion de ces risques afin d’apaiser l’inquiétude croissante des internautes

CONCLUSION DU CHAPITRE 2

175. Le *spamming* évolue dans un environnement socio-économique conflictuel où les données nominatives sont tiraillées entre la nécessité pour les « spammeurs » d'en collecter le plus grand nombre possible et l'aspiration des titulaires à retrouver un contrôle sur leurs données qui paraît leur échapper. Les questions relatives à l'identité de la personne, à sa traduction numérique et à la maîtrise de ses données, c'est-à-dire la manière dont la personne les utilise, les contrôle et les communique ou non deviennent un enjeu majeur au regard des risques inhérents à cette « marchandisation » des données. Ce conflit entre des intérêts opposés s'illustre également à travers la revendication des « spammeurs » à la liberté d'expression commerciale et l'aspiration des « spammés » à un droit à être laissé tranquille. Dans ce contexte, la mise en place d'un système de protection équilibré où coexisteraient de façon harmonieuse intérêts collectifs et intérêts privés [440] apparaît comme un véritable défi pour les législateurs. Ils doivent œuvrer à trouver un équilibre d'une part, entre le nécessaire accès à cette richesse informationnelle et l'impérative limitation de son usage afin d'éviter tout abus [441] et d'autre part, entre la préservation de l'activité de prospection commerciale et la protection des « spammés » contre l'envahissement de ces courriers électroniques non sollicités.

[440] À ce titre, Henri COMTE estime que la conciliation de ces impératifs n'est pas impossible voire nécessaire à la préservation de chacun des deux : « *le rapport entre les intérêts collectifs liés à l'expansion des NTI et la préservation de la vie privée n'est pas à penser sur le registre du conflit mais sur celui de la complémentarité, voire de la synergie. Autrement dit elle repose sur l'idée centrale que sans protection de la vie privée efficace et à un niveau élevé, le développement des NTI est voué à s'essouffler, voire à s'interrompre, par généralisation de la méfiance à son égard* » (Henri COMTE, « Comment préserver les intérêts collectifs sans attenter à la vie privée ? L'action de l'Union européenne », *in* Marie-Christine PIATTI, *Les libertés individuelles à l'épreuve des NTIC*, *op. cit.*, spéc. pp.77-78). – Plus généralement, Jean FRAYSSINET explique que « *la protection des droits et libertés fondamentales du consommateur peut entrer en conflit avec les intérêts des fournisseurs de biens et de services, des collecteurs et vendeurs des données personnelles qui considèrent que celles-ci sont leur propriété en raison de l'investissement, de la liberté du commerce et de l'industrie, de l'utilité fonctionnelle des données* », (« Nouvelles technologies de l'information et de la communication et protection des libertés des consommateurs », art. préc., spéc. p. 38).

[441] Cette difficile recherche d'équilibre rejoint les observations de Pierre Trudel qui, réfléchissant sur la question de la conciliation du développement technologique avec les impératifs socio-juridiques, notamment celui de la protection de la vie privée, souligne la complexité de cette entreprise dans les environnements électroniques : « *La délocalisation de l'information, sa grande fluidité, voire son insaisissabilité, son caractère multimédiatique (données, voix, son, image), son intangibilité, sa nature souvent interactive, la multiplicité des acteurs impliqués dans l'opération télématique et, surtout,* […] *le caractère irrémédiablement international des réseaux de communication participent à la difficulté de procéder à un arbitrage efficace, opérationnel et harmonieux des intérêts en jeu* ». Pierre TRUDEL (sous la dir.), *Droit du cyberespace*, Thémis, 1997, p. 11 et s.

176. Des risques à maîtriser. Par le biais des nouvelles technologies, la numérisation des données a favorisé leur circulation et leur échange. Cette évolution n'est toutefois pas sans risque puisque l'accessibilité aux données a, dans le même temps, accru leur vulnérabilité. Les « spammeurs » ont bien compris les enjeux économiques qui s'attachent à ces données. Profitant des failles techniques existantes, ils n'hésitent pas à recourir à des procédés de collecte de plus en plus performants pour intensifier les collectes de données. Une fois les adresses électroniques capturées, les « spammeurs » n'ont plus qu'à « bombarder » d'*e-mails* non sollicités les messageries auxquelles se rattachent ces dernières. À ce risque pesant sur les données s'ajoute l'évolution inquiétante du *spamming*. En effet, cette pratique n'est plus limitée au seul courrier électronique mais a également envahi les services de messagerie instantanée, les *blogs* ou encore les réseaux sociaux tels que *Facebook* ou *Twitter* et gagne désormais les téléphones mobiles de nouvelle génération qui permettent d'accéder aux *e-mails*. Surtout, nous avons pu constater que le *spamming* apparaît comme une pratique de plus en plus malveillante et dangereuse qui accroît la nécessité d'assurer une protection efficace des victimes. Les *spams* ne sont plus en effet de simples messages non sollicités qui exaspèrent leurs destinataires, mais sont devenus les vecteurs de propagation de multiples menaces, en facilitant la diffusion de virus et autres logiciels malveillants ou en s'associant à des opérations frauduleuses comme le *phishing*.

177. La lutte anti-*spam*, un véritable défi pour les législateurs. Pour répondre à cet impératif de protection des « spammés » et de leurs données, le recours aux dispositifs techniques de protection est apparu comme une initiative nettement insuffisante pour lutter contre ce phénomène dans son ensemble. En effet, au-delà des menaces d'ordre technique qui remettent en cause la fiabilité et l'efficacité des services de messagerie électronique et plus largement, qui inspirent la méfiance envers les communications électroniques, le *spamming* porte atteinte aux droits et libertés des internautes et rend ainsi indispensable l'intervention légale. Au regard des divers dangers constatés, le législateur doit s'efforcer de mettre en place un régime de protection fort. Tout d'abord, au bénéfice des titulaires de données nominatives afin de leur garantir un meilleur contrôle sur leurs données grâce à un encadrement rigoureux des opérations de collecte et de traitement. Ensuite, au profit des « spammés » eux-mêmes afin que ces derniers puissent faire respecter leur droit à être laissé tranquille. La poursuite de cette étude conduit donc naturellement à analyser comment les

législateurs ont appréhendé ces différentes problématiques afin d'apprécier si le dispositif législatif en vigueur apparaît à la hauteur des attentes et des menaces identifiées.

TITRE SECOND : DES LÉGISLATIONS SPÉCIALES FRAGILES

178. Une triple problématique. Tel qu'il a été précédemment exposé, la circulation des données à caractère personnel les expose potentiellement à une collecte massive destinée aux traitements les plus divers [442]. À cet égard, le *spamming* illustre parfaitement les menaces qui pèsent sur ce type de données, en particulier sur les adresses électroniques des internautes, leur collecte étant l'opération préalable indispensable à l'envoi de *spams* [443]. Cette pratique renferme dès lors deux problématiques intervenant à deux stades distincts dans son processus : en amont, se pose la question de la licéité de la collecte et de l'utilisation de ces données ; en aval, celle de la licéité de l'envoi proprement dit. Par ailleurs, en raison de la dimension internationale du *spamming*, cette double problématique ne peut être traitée dans un contexte exclusivement national, l'effectivité de la protection des « spammés » dépendra nécessairement d'une certaine harmonie entre les lois étrangères destinées à traiter d'un même problème. Notre étude nous conduira ainsi à étudier les différentes obligations fixées par les législations nationales afin de déterminer d'une part, à partir de quel moment la collecte puis l'utilisation des données à caractère personnel sont considérées comme irrégulières et d'autre part, comment les législateurs sont intervenus pour réglementer le *spamming*. Pour cela, la confrontation des systèmes juridiques français et américain sera particulièrement instructive puisqu'elle mettra en exergue les divergences qui caractérisent leur législation respective, tant en matière de protection des données à caractère personnel (Chapitre 1er.) qu'en ce qui concerne les dispositions régissant spécifiquement la pratique du *spamming* (Chapitre 2.), faisant ainsi douter de leur effectivité lorsque le contentieux présente une dimension internationale.

[442] V. *supra :* n° 84 et n° 147 et s.
[443] Sur l'appartenance des adresses électroniques à la catégorie des données à caractère personnel, v. *infra* : n° 186.

CHAPITRE PREMIER : DES LOIS DE PROTECTION DES DONNÉES INCOMPLÈTES FACE AUX MENACES DU *SPAMMING*

179. La question de l'efficacité des lois face au *spamming*. La collecte des adresses électroniques et leurs utilisations par les « spammeurs » conduisent à s'interroger sur la licéité de ces opérations au regard des différentes règles régissant la protection des données à caractère personnel. À cette occasion, il s'agira de déterminer si le « spammeur » est soumis au respect d'exigences équivalentes en termes de collecte et de traitement des données quel que soit le pays d'émission des *spams* et quelles sont les garanties offertes aux titulaires de ces données. Dans cette perspective, les prochains développements s'attacheront à une analyse comparée des systèmes législatifs français et américain afin d'évaluer leur cohérence, le régime adopté reflétant l'importance accordée à la protection des données. La comparaison des réponses légales offertes par chacun d'eux permettra de saisir leurs spécificités et les contrastes qui risquent de poser de sérieuses difficultés en termes d'effectivité. En effet, le *spamming* s'inscrivant le plus fréquemment dans un cadre extraterritorial, une lutte optimale contre cette pratique commande une certaine harmonie entre les législations étrangères. Or, nous constaterons de façon regrettable que cette exigence est loin de se vérifier au regard des oppositions existant entre les lois en vigueur. Nous verrons que le système européen, et notamment le système français, adopte une approche dite « systématique » [444], caractérisée par une législation générale, applicable à presque toutes les données, quels que soient la catégorie de fichiers et les responsables des fichiers concernés. Les États-Unis, quant à eux, adoptent au contraire une approche qualifiée de « sectorielle » [445]. Au-delà de cette opposition, nous mettrons en évidence que chacun de ces systèmes reste incomplet face aux menaces du *spamming* : malgré une protection française uniforme, le système juridique adopté demeure à renforcer pour assurer une lutte efficace contre le *spamming* dans un contexte national mais aussi international (Section I.) ; l'absence d'un système de protection générale des données laisse apparaître une législation contrastée qui reste largement à uniformiser (Section II.).

[444] Notion empruntée à Robert GELLMAN, avocat près la Cour suprême de Pennsylvanie et expert-conseil en matière de protection des données (« L'approche américaine : la régulation par le congrès, le marché et le juge » *in Informatique : servitude ou libertés ?*, Colloque organisé par la CNIL et l'université Panthéon-Assas-Paris II, Sénat, 7 et 8 nov. 2005, disponible sur : http://www.senat.fr/colloques/colloque_cnil_senat/colloque_cnil_senat.html.

[445] *Id.*

SECTION I. EN FRANCE, UNE PROTECTION UNIFORME À RENFORCER

180. La protection des données, une question primordiale en France. En réponse à la nécessité d'apaiser l'inquiétude générale suscitée par la multiplication des fichages opérés par l'État ou les entreprises, la France a été l'un des premiers États à introduire dans sa législation des dispositions protectrices des données à caractère personnel [446]. Elle s'est en effet dotée dès 1978 de la loi n° 78-17 relative à l'Informatique, aux fichiers et aux libertés , dite « loi IFL » [447], dont l'influence sur les régimes de protection des données postérieurs a poussé certains à la considérer comme « *un modèle* » [448]. Elle a en particulier fortement inspiré la directive n° 95/46/CE relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données du 24 octobre 1995 [449] qui prévoyait des principes destinés à encadrer la collecte et le traitement de ces données sur l'internet, principes qui seront repris par la loi française de transposition du 6 août 2004 [450].

[446] L'Allemagne a adopté en 1970 la première loi relative au traitement automatisé des données nominatives suivi peu après par la Suède en 1973.

[447] Loi n° 78-17 du 6 janvier 1978 relative à l'Informatique, aux fichiers et aux Libertés, J.O. du 7 janvier 1978, p. 227 et s. et rectificatif, J.O. du 25 janvier 1978. Selon Jean FRAYSSINET, cette loi s'est révélée « *nécessaire* » en raison du développement de l'informatique mais aussi de la création de fichiers manuels qui peuvent tout autant constituer un danger pour les droits et libertés (*Informatique, fichiers et libertés* (préf. Jacques FAUVET), Litec, 1992, spéc. pp. 5-6.). – Pour une étude générale de cette loi, v. not. Pascal ANCEL, « La protection des données personnelles : Aspects de droit privé français », *RIDC* 1987-3, p. 609 et s. – Henri DELAHAIE et Félix PAOLETTI, *Informatique et libertés*, La Découverte, coll. *Repères*, Paris, 1987. – Jean FRAYSSINET, *Informatique fichiers et libertés, op. cit. ;* « La loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés », *Rev. dr. publ.* juill.-août 1978, n° 94/2, p. 1094 et s. ; « La loi du 6 janvier 1978, Informatique, fichiers et libertés : Présentation pédagogique et synthétique », *RRJ* 1987-1, p. 191 et s. – Annie GRUBER, « Le système français de protection des données personnelles », *LPA* 4 mai 2007, n° 90, p. 4 et s. – André de LAUBADERE, « Loi relative à l'informatique, aux fichiers et aux libertés », *AJDA* mars 1978, n° 3, p. 146 et s. – André LUCAS, Jean DEVEZE et Jean FRAYSSINET, *Droit de l'informatique et de l'internet, op. cit.*, spéc. pp. 99 et s. – Herbert MAISL, « La maîtrise d'une interdépendance (commentaire de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés), *JCP* 1978, éd. G., I. 2891.

[448] Jean FRAYSSINET souligne que « *la principale originalité de la loi du 6 janvier 1978 est d'établir pour la première fois un véritable régime juridique de l'information nominative fichée grâce à des techniques traditionnelles ou traitées automatiquement grâce aux outils informatiques* » (*Informatique, fichiers et libertés, op. cit.*, spéc. n° 110, p. 47).

[449] Dir. préc. – La réglementation européenne en matière de protection des données à caractère personnel s'est réellement construite lors de l'adoption de la directive 95/46/CE précitée. Le Conseil de l'Europe s'est engagé à son tour dans une politique de protection des données nominatives avec la signature à Strasbourg, le 28 janvier 1981, de la Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel » (*S.T.E.* n° 108, Strasbourg, 28 janv. 1981, J.O. du 20 novembre 1985, p. 13436 et s.). Laissant toutefois le soin aux législateurs nationaux d'adopter les mesures nécessaires à son application (art. 4), cette convention n'a donc pas d'effet direct en droit interne. Elle vise à concilier le respect de la vie privée et la libre circulation de l'information. Par la suite, plusieurs directives ont été adoptées : les directives 97/66/ CE, 97/7/ CE, 2000/31/CE, 2002/58/ CE (sur ces directives, v. *infra*).

[450] Loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, J.O. n° 182 du 7 août 2004, p. 14063 et s. – Sur le projet de loi, v. not. Sabine LIPOVETSKY et Audrey YAYON-DAUVET, « Le devenir de la protection des données personnelles sur Internet », *Gaz. Pal.* 13 sept. 2001, 2, p. 2 et s. – Ariane MOLE, « Projet de loi informatique et libertés : le miroir à " deux faces " », *Gaz. Pal.* 16 oct. 2001, n° 289, p. 4 et s. – V. ég. la saisine du Conseil constitutionnel avant la

181. Objectif de l'étude. La plupart des activités de *spamming* implique la collecte préalable d'adresses électroniques. Or, nous verrons que ces adresses étant des données à caractère personnel au sens de la loi IFL, leur utilisation est strictement encadrée (§ 1.). Toutefois, la confrontation des dispositions légales à la réalité du *spamming* démontrera que le « spammeur » opère en parfaite violation de la loi (§ 2.). Face aux multiples manquements auxquels il se livre, il conviendra d'envisager sa condamnation. À ce titre, la loi de 1978, complétée en 2004, a inséré dans le Code pénal une série d'incriminations venant sanctionner les atteintes à la loi IFL. Il conviendra d'évaluer l'effectivité de ce volet pénal à la lumière des sanctions fixées par les textes et des peines prononcées. Cette analyse est essentielle puisque si « [l]*a sanction est indispensable à la crédibilité d'un dispositif qui sans elle, peut être considéré comme de la poudre aux yeux* » [451], encore faut-il que des condamnations dissuasives soient prononcées, sous peine de faire du dispositif répressif un simple vœu chimérique [452]. Malgré un renforcement des peines par la loi de 2004, le bilan de sa mise en œuvre reste très décevant et conduit à déplorer que son effectivité apparaisse largement illusoire (§ 3.)

§ 1. LE *SPAMMING*, UNE PRATIQUE SOUMISE AU RESPECT DE LA LOI INFORMATIQUE, FICHIERS ET LIBERTÉS

182. La loi française s'applique « aux traitements automatisés de données à caractère personnel, ainsi qu'aux traitements non automatisés de données à caractère personnel contenues ou appelées à figurer dans des fichiers », à l'exception des traitements relevant du strict exercice du droit à la vie privée [453]. Il sera démontré que toute activité de spamming s'inscrit dans le champ d'application de cette loi, d'une part parce que les données exploitées par le « spammeur » sont des données à caractère personnel (A.) et d'autres part

promulgation de la loi (Cons. const., DC n° 2004-499 du 29 juill. 2004, J.O. du 7 août 2004, p. 14087, *Rec. const*., p. 126 ; *Comm. com. électr*. nov. 2004, comm. 146, p. 35 et s., note A. Lepage). – Pour une analyse approfondie de cette loi, v. not. Jean FRAYSSINET, « La loi relative à l'Informatique, aux fichiers et aux libertés, modifiée par la loi du 6 août 2004 : continuité et/ou rupture ? », *RLDI* oct. 2005, n° 267, p. 50 et s. ; « Trente ans après, la Loi " Informatique et Libertés " se cherche encore », *RLDI* janv. 2008, n° 1157, p. 69 et s. – Alexandre MAITROT DE LA MOTTE, « La réforme de loi informatique et libertés et le droit au respect de la vie privée », *AJDA* 2004, p. 2269 et s. – Pour une approche pragmatique des impacts de la loi, v. not. Valérie BOCCARA, « Loi " informatique et libertés " : des sanctions fortes, des risques accrus », *LPA* 16 févr. 2005, n° 33, p. 3 et s.

[451] André VITALIS, *Informatique, Pouvoir et Libertés*, *op. cit,* spéc. p. 203, citant Pierre TRUDEL, « Éléments de droit et de déontologie de l'information administrative », *in Les implications socio-professionnelles des changements technologiques*, Université du Québec, 1985.

[452] André VITALIS, *Informatique, Pouvoir et Libertés*, *ibid., loc. cit.*

[453] Art. 2, al. 1er loi n° 2004-801. – Sur cette exception, v. not. Jean FRAYSSINET, *Informatique fichiers et Libertés, op. cit.*, spéc. n° 107, pp. 42-43. – André LUCAS, *Le droit de l'informatique*, P.U.F., coll. *Thémis Droit*, Paris, 1987, spéc. note 8, p. 34.

parce que l'ensemble des opérations réalisées sur ce type de données s'analyse comme un traitement au sens de la loi (B.).

A. LA COLLECTE DE DONNEES A CARACTERE PERSONNEL PAR LE « SPAMMEUR »

183. À l'instar de l'adresse postale, les adresses électroniques se révèlent indispensables à l'envoi de *spams* par courrier électronique. Ces données sont qualifiées, sans difficulté, de données à caractère personnel au sens de la loi IFL (1.). Toutefois, ces dernières ne sont plus les seules convoitées par les « spammeurs ». Le *spamming* s'est en effet progressivement diversifié, le « spammeur » utilisant d'autres formats de messages tels que les SMS ou de MMS. Dans ces hypothèses, l'envoi de *spams* est subordonné à la collecte des numéros de téléphone mobile des destinataires. La classification de ces données dans la catégorie des données à caractère personnel a été clairement rappelée à plusieurs reprises par la CNIL [454] et n'appelle aucune remarque particulière. En revanche, un autre cas retiendra plus particulièrement notre attention. L'accessibilité largement facilitée aux services de l'internet depuis les téléphones mobiles a accru leur utilisation à diverses fins et notamment pour l'envoi de *spams*. Les « spammeurs » ont commencé à utiliser le protocole de communication sans fil *Bluetooth*. L'existence de ces nouveaux *spams*, désignés par l'expression « *Blue spam* », est subordonnée à la collecte de données traitées par *Bluetooth* [455]. Cette hypothèse conduit à s'interroger sur la nature juridique de ce type de données afin de déterminer si elles ont vocation à bénéficier du régime de protection de la loi IFL (2.).

1. L'adresse électronique, une donnée à caractère personnel

184. Information nominative et donnée à caractère personnel : substitution et incidences. À titre préliminaire, l'analyse des dispositions de la nouvelle loi de 2004 permet de constater l'abandon des termes d'« information nominative » utilisés par la loi de 1978 [456] au profit de ceux de « donnée à caractère personnel ». Ce constat mène tout naturellement à s'interroger sur la portée de cette évolution terminologique et notamment à déterminer si cette dernière traduit une orientation nouvelle, attribuant un sens nouveau aux données

[454] V. *supra :* n° 185.
[455] V. *supra :* n° 100.
[456] Art. 4 loi n° 78-17.

protégées par la loi française. Nous prendrons le parti de répondre par la négative. En effet, si la référence à la notion plus neutre de données à caractère personnel permet de l'adapter aux réalités technologiques [457], ces deux notions (donnée à caractère personnel et information nominative) restent synonymes [458]. La question se pose de façon identique pour les « données » et les « informations » : peuvent-elles être indifféremment utilisées ? la réponse est positive. En effet, l'emploi de termes distincts renvoie seulement à des étapes différentes du processus de transformation d'un état de matière première à un produit fini. À cet égard, il est traditionnellement considéré que « *l'information fait figure de produit fini dont les données seraient la matière première* » [459], mais la pratique semble parfois inverser la tendance et considérer l'information comme la matière brute à partir de laquelle se construiraient les données. En tout état de cause, que la donnée soit considérée comme l'élément générateur de l'information ou sa résultante, cela n'a pas d'impact sur notre démonstration. Tout au long de ces développements, nous utiliserons donc alternativement les notions de « donnée » et d'« information ».

185. Une acception large des données à caractère personnel. La loi de 2004 consacre une définition très large des données à caractère personnel : entre dans cette catégorie « *toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres* » [460]. En fixant ainsi un champ d'application

[457] Les évolutions technologies favorisent un élargissement constant du champ de « *l'indirectement nominatif* » (v. notamment le débat sur l'adresse IP (v. *infra* : n° 187)).

[458] En ce sens, v. Jean FRAYSSINET, favorable à cette tendance énonce que « *La convention du Conseil de l'Europe utilise la notion de "donnée à caractère personnel", compatible avec la notion d'"informations nominatives"* » (*Informatique fichiers et libertés, op. cit.*, spéc. n° 84, p. 35). – Frédéric LESAULNIER, *L'information nominative*, thèse préc. n° 15 et s., p. 29 et s

[459] En ce sens, v. Frédéric LESAULNIER, *L'information nominative*, thèse préc., spéc. n° 16, p. 30. – Pour justifier une « *utilisation alternative* » de ces deux termes, Nathalie MALLET-POUJOL relève, dans le domaine des banques de données, « *la proximité sémantique entre information et donnée* » *:* « *Quand bien même la donnée ne saurait qu'un des modes, parmi d'autres, de représentation de l'information, elle en est le mode privilégié pour les banques de données. Or, l'information nous intéresse, en l'espèce, conjointement en sa dimension d'élément de connaissance et de représentation de cet élément de connaissance. C'est avec sa formalisation en donnée que l'information est collectée et traitée par la banque de données. Information et donnée deviennent synonymes dans ce contexte* » (*Commercialisation des banques de données*, CNRS Éditions, 1993, spéc. p. 19).

[460] Art. 2, al. 2 loi n° 2004-801. – Rappr. de l'article 4 loi n° 78-17 : « *sont réputées nominatives* […] *les informations qui permettent, sous quelque forme que ce soit, directement ou non, l'identification des personnes physiques auxquelles elles s'appliquent* » et de l'article 2 a) dir. 95/46/CE : « *est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale* ». – Analysant cette disposition, Jean FRAYSSINET, précise que : « [l]*es caractéristiques subjectives et objectives de l'information nominative ne sont pas à considérer. Peu importe si l'information est sensible ou non, protégée ou facilement accessible, publique ou confidentielle, aisée ou non à comprendre ; peu importe son sens et son objet, si elle concerne une personne mineure ou majeure. La forme des informations est indifférente : caractères alphanumériques directement lisibles ou codées (caryotype génétique)* [sic]), image fixe ou animée (dessin, photo, film, bande-vidéo), son, (voix), etc. » (*Informatique fichiers et libertés, op. cit.*, spéc. n° 81, pp. 34-35). – La CNIL a pour sa part également consacré une conception large des données nominatives (CNIL, Délibération 80-10 du 1er avril 1980, Rapport annuel 1980, et CNIL 6ème

extrêmement étendu, la loi reflète la volonté du législateur d'embrasser le maximum de données nominatives afin d'assurer une protection efficace de ces dernières face aux multiples atteintes dont elles sont devenues la cible. Cette acceptation large est confirmée au regard des méthodes auxquelles il est possible d'avoir recours pour déterminer si une personne est identifiable. La loi précise en effet qu'« *il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne* » [461]. Il s'agit donc de toute information qui permet à la fois de reconnaître une personne et de l'individualiser [462]. Cela rejoint ainsi les propos du professeur Jean FRAYSSINET qui énonce très clairement qu'« [à] *partir du moment où l'information peut être rapportée à la personne concernée, la condition d'identification est remplie. Le rapport peut être direct (nom, prénom…) ou indirect (utilisation d'un identifiant codé comme le numéro de sécurité sociale, lien entre le numéro d'immatriculation du véhicule et le propriétaire, le numéro de téléphone et l'abonné, le numéro de carte de crédit et le porteur, etc.)* » [463].

186. L'adresse électronique, une donnée nominative. Si l'adresse électronique n'identifie pas l'internaute directement mais seulement sa boîte aux lettres électroniques, celle-ci fournit de nombreuses informations sur son titulaire dans la mesure où elle contient le plus souvent son nom, voire son prénom mais aussi son pays d'établissement, son lieu de travail ou encore son fournisseur de messagerie et/ou d'accès internet. À titre d'exemple, l'adresse électronique de type « pierre.marchand@coe.int » révèle non seulement ses prénom et nom mais aussi son lieu de travail (le Conseil de l'Europe). L'adresse du type « pierre.marchand@free.fr » indique, quant à elle, que Pierre Marchand a souscrit un abonnement Internet auprès du FAI, FREE, et que son lieu de résidence est situé en France. Cette réalité a ainsi conduit la CNIL à reconnaître l'adresse électronique comme une donnée à caractère personnel. En effet, dès la première page de son rapport de 1999 intitulé *Le publipostage électronique et la protection des données personnelles*, la Commission énonce sans ambiguïté que : « *Au regard des législations de protection des données personnelles, une adresse électronique est évidemment une information nominative : directement nominative lorsque le nom de l'internaute figure dans le libellé de l'adresse ; en tout état de cause, toujours indirectement nominative dans la mesure où toute adresse électronique est*

rapport d'activité p. 44 et s. et p. 50). – CE, 7 juin 1995, *Caisse régionale de Crédit Agricole de la Dordogne et Caisse nationale de Crédit Agricole*, *RJDA* 1995, n° 1452 ; *LPA* 13 avr. 1998, n° 44, pp. 9-10, obs. J.-P. M.

[461] Art. 2, al. 2 loi n° 2004-801.

[462] Sur la fonction d'identification des données à caractère personnel, v. *supra* : n° 58.

[463] Jean FRAYSSINET, *Informatique fichiers et libertés*, *op. cit.*, spéc. n° 83, p. 35.

associée à un nom et à une adresse physique » [464]. De même, la jurisprudence française a adopté de façon constante cette analyse dans des litiges où les traitements de données à caractère personnel, et notamment d'adresses électroniques, violaient les obligations posées par la loi IFL [465].

2. La question de la nature juridique des données *Bluetooth*

187. Les données *Bluetooth*, des données à caractère personnel ? La question qui se pose est alors celle de savoir si les données techniques traitées dans le cadre de ce protocole de communication, à savoir l'adresse physique de l'interface du portable (adresse " MAC ") et l'identifiant *Bluetooth* du téléphone portable sont des données à caractère personnel. Lors de la séance plénière en date du 11 septembre 2008, la CNIL s'est clairement prononcée par l'affirmative [466]. Deux raisons peuvent venir au soutien de la position de cette dernière. D'un point de vue technique tout d'abord, il convient de préciser que chaque terminal mobile possède une adresse MAC unique, c'est-à-dire une adresse apparaissant sous une forme alphanumérique hexadécimale, du type <5A:DD:56:F2:EA:13>, attribuée par le constructeur et qui désigne de façon unique une machine du réseau local. Chaque téléphone

[464] Cécile ALVERGNAT (Rapport CNIL présenté par), *Le publipostage électronique et la protection des données personnelles*, 14 oct. 1999, rapport préc. – CNIL, *Rapport d'activité 1999*, rapport préc., spéc. pp. 107-108.

[465] Cass. crim., 14 mars 2006, *Fabrice X. c/ Ministère Public*, pourvoi n° 05-83.423, *Bull. crim.* 2006, n° 69 ; *Comm. com. électr*. sept. 2006, comm. 131, p. 43 et s., note A. Lepage ; *D.* 2006, p. 1066 ; *JCP* 2006, éd. G., IV. 1819, *RLDI* mai 2006, n° 471, p. 34 et s., note J. Le Clainche et *RLDI* juin 2006, n° 498, p. 28 et s., note Ph. Belloir (La Cour de cassation reprend ainsi le raisonnement des juges de première instance (TGI Paris, 17e ch., 7 déc. 2004, *Ministère Public c/ Fabrice H.*, *RLDI* mai 2005, n° 141, p. 28 et s., note J. Le Clainche) qui avaient énoncé que les adresses électroniques permettaient « *en règle générale d'identifier la personne physique auxquelles elles s'appliquent, soit directement, quand le nom et le prénom de cette personne figurent en toute lettre dans l'adresse, soit indirectement* ». – V. ég. plus récemment TGI Paris, 31e ch., 18 sept. 2008, *Éditions Neressis c/ Arkadia, Stéphane V. C., Comm. com. électr.* janv. 2009, n° 1, comm. 10, p. 48 et s., note Éric A. Caprioli (les magistrats ont considéré, à propos notamment des adresses électroniques, que le délit de collecte de données à caractère personnel par un moyen frauduleux est constitué dès lors que « *les données des particuliers ont été collectées sur la partie confidentielle du site qui n'était pas accessible au public* »). – *A contrario*, les coordonnées apparaissant « *sous la forme suivante : tableaublanc2005@wanadoo.fr* […] *ne permett*[ent] *plus l'identification de l'intéressée* » (TGI Paris, 17e ch., 2e sect., 10 juill. 2002, *Anne D. c/ Société Wanadoo*, disponible sur : http://legalis.net/jurisprudence-decision.php3?id_article=137).

[466] CNIL, « Pas de publicité via *Bluetooth* sans consentement préalable », 13 nov. 2008, disponible sur : http://www.cnil.fr/es/la-cnil/actu-cnil/article/article/pas-de-publicite-via-bluetooth-sans-consentement-prealable/?tx_ttnews[backPid]=91&cHash=dd9280c396). – À l'occasion d'une demande de conseil auprès de la CNIL de la société MOBINEAR, spécialisée dans la création, l'édition et la commercialisation de logiciels par téléphone mobile ou ordinateur, et qui intéressait une technologie qu'elle avait développée et permettant d'établir des communications avec des terminaux de mobile au standard *Bluetooth*. À cette occasion, la CNIL a apporté certaines précisions quant à la qualification de données à caractère personnel en cette matière : « *S'agissant de l'identifiant Bluetooth, il est possible à tout utilisateur de modifier cet identifiant et de le personnaliser selon sa convenance en y intégrant des données à caractère personnel (par exemple, le nom du titulaire du téléphone). L'adresse MAC* [quant à elle] *constitue également une donnée à caractère personnel en ce qu'elle permet d'identifier un utilisateur sur le réseau ; concerne une personne physique ; peut être rattachée à une adresse IP* » (Courrier d'Alex TURK, Président de la CNIL, adressé à Christian CHABREBRIE, PDG de la société MOBINEAR, 23 oct. 2008, disponible sur : http://www.mobinear.com/corporate/MobiNear_BlueNFC_CNIL_OK_20081027.pdf).

dispose également d'un identifiant *Bluetooth* affecté selon le modèle du téléphone (SAMSUNG Z360, par exemple). Ces données, accessibles *via Bluetooth*, sont personnalisables, l'utilisateur pouvant préciser les données de son choix comme notamment son nom, son pseudonyme, son adresse postale physique ou numérique ou encore son numéro de téléphone. D'un point de vue juridique ensuite, les difficultés de qualification des données traitées par *Bluetooth* rejoignent le célèbre débat qui s'est engagé, dans le cadre du contentieux relatif à la répression pénale du téléchargement illégal [467], sur le point de savoir si l'adresse IP constitue une donnée à caractère personnel [468]. Si la CNIL [469] et le groupe de l'article 29 se sont clairement prononcés en faveur de cette qualification, la juridiction judiciaire reste divisée [470], la Cour de cassation ne s'étant pas clairement prononcée sur cette

[467] Le contexte est le suivant : des agents d'un organisme de protection des droits d'auteurs (art. L. 321-1 et L. 331-1 du Code de la propriété intellectuelle) avaient collecté l'adresse IP d'internautes mis en cause pour le piratage d'œuvres musicales et audiovisuelles et l'avaient transmise aux services de police qui, après avoir interrogé leur FAI, étaient parvenus à identifier les propriétaires des ordinateurs incriminés. Pour leur défense, ces internautes avaient argué de la nullité de la procédure déclenchée à leur encontre pour violation de la loi IFL. Selon ces derniers, l'adresse IP constitue une donnée à caractère personnel dont la collecte de cette donnée est subordonnée à leur consentement préalable.

[468] CNIL, délibération n° 2006-294 du 21 décembre 2006 autorisant la mise en œuvre par l'Association de Lutte contre la Piraterie Audiovisuelle (LPA) d'un traitement de données à caractère personnel ayant pour finalité principale la recherche des auteurs de contrefaçons audiovisuelles. – Éric BARBRY et Isabelle POTTIER, « La CNIL et le rapport Olivennes luttent contre le téléchargement illicite, *Gaz. Pal.* 20-22 janv. 2008, n^{os} 20-22, p. 17 et s.

[469] G29, Avis n° 4/2007 sur le concept de données à caractère personnel, 01248/07/FR, WP 136, 20 juin 2007, spéc. pp. 18-19, disponible sur : http://www.cnpd.public.lu/fr/publications/groupe-art29/wp136_fr.pdf.

[470] V. par ex. TGI Montauban, 9 mars 2007, *SCPP c/ Marie-Thérèse O., inédit*, disponible sur le site <legalis.net>. – CA Paris, 13^{e} ch., sect. A, 15 mai 2007, *S. c/ Ministère Public et autres*, RG n° 06/01954, Jurisdata : 2007-336454, *Comm. com. électr.* déc. 2007, comm. 144, p. 32 et s., note C. Caron. – CA Paris, 13^{e} ch., sect. B, 27 avr. 2007, *Juris-Data* n° 2007-338935 (« *cette série de chiffres* […] *ne constitue en rien une donnée indirectement nominative relative à la personne dans la mesure où elle ne se rapporte qu'à une machine, et non à l'individu qui utilise l'ordinateur pour se livrer à la contrefaçon* »). – CA Paris, 3^{e} ch. instr., 28 mai 2008, RG n° 2007-01064, *Dr. pénal* déc. 2008, Étude 27, p. 24 et s., note L. Flament (« *le relevé de l'adresse IP de l'ordinateur ayant servi à l'infraction entre dans le constat de sa matérialité et pas dans l'identification de son auteur ; que cette série de chiffres ne constitue pas une donnée indirectement nominative relative à la personne dans la mesure où elle ne se rapporte qu'à une machine et non à la personne qu'elle utilise ; que la consultation des sites accessibles au public ne permet que de déterminer que le fournisseur d'accès internet mais aucunement l'utilisateur de l'ordinateur en cause* »). – CA Paris, 12^{e} ch., 1er févr. 2010, *Cyrille S. c/ Sacem, SDRM*, disponible sur le site <legalis.net> (« *les constatations de l'agent assermenté ayant abouti au relevé de l'adresse " IP " de l'ordinateur ayant servi à l'infraction, ne constituent pas davantage un traitement de données à caractère personnel relatives à des infractions relevant de l'article 9-4 de la loi précitée, le dit relevé entrant dans le constat de la matérialité de l'infraction et pas dans l'identification de son auteur* »). – *Contra* TGI Saint-Brieuc, 6 sept. 2007, *Ministère Public, et al. c/ P., inédit, RLDI* oct. 2007, n° 1028, p. 26 et s., obs. L. Costes et J.-B. Auroux. – TGI Paris, ord. réf., 24 déc. 2007, *Techland c/ France Télécom et autres, RLDI* févr. 2008, n° 1167, p. 27 et s., note L. Costes et J.-B. Auroux (« *il ne peut être sérieusement contesté le fait que les adresses* […] *IP collectées* […] *constituent des données à caractère personnel* »). – CA Rennes, 3^{e} ch. crim., 22 mai 2008, *SACEM, SDRM et Ministère Public c/ Cyrille S.*, RG n^{o} 07/01495. – CA Rennes, 3^{e} ch., 23 juin 2008, *L. T. c/ Ministère public*, RG n^{o} 07/01021, *RLDI* juill. 2008, n^{o}40, p. 17 et s., note L. Costes. – Le Conseil d'État a également implicitement admis cette qualification (CE, 23 mai 2007, n° 288149, *Sté des auteurs compositeurs et éditeurs de musique et a., Juris-Data* n° 2007-071900 ; *Comm. com. électr.* juill. 2007, comm. 90, p. 28 et s., note C. Caron ; *JCP* 2007, éd. G, I. 176 ; *Propr. intell.* juill. 2007, n° 24, pp. 334-335, obs. J.-M. Bruguière ; *Expertises* 2007, n° 316, pp. 263-264, note L. Walker ; *Légipresse* juill.-août 2007, III, n° 243, III, p. 141 et s., note J. Frayssinet).– Cette solution rejoint ainsi la position de la juridiction communautaire qui a considéré l'adresse IP comme une donnée à caractère personnel (CJCE, 29 janv. 2008, *Productores de Música de España (Promusicae) c/ Telefónica de España SAU*, Aff. C-275/06, *JCP* 2008, éd. G, II. 10099, note E. Derieux ; *Comm. com. électr.* mars 2008, comm. 32, p. 25 et s., note C. Caron ; *D.* 2008. AJ, p. 480, obs. J. Daleau ; *RTD com.* 2008, p. 302 et s., obs. F. Pollaud-Dulian ; 19 févr. 2009, *LSG c/ Tele 2 Telecommunication*, aff. C-557/07, *Dalloz Actualités* 13 mars 2009, comm. J. Daleau.

question [471]. Quant à la doctrine, celle-ci apparaît également partagée [472]. Au regard des derniers travaux parlementaires, cette question est peut être sur le point d'être tranchée [473]. En effet, les parlementaires ont récemment appelé de leurs vœux une clarification du statut de l'adresse IP dans une proposition de loi déposée en 2009 [474]. Si cette dernière venait à être définitivement adoptée, l'adresse IP serait juridiquement qualifiée de donnée à caractère personnel. La reconnaissance officielle des données traitées par *Bluetooth* en tant que données à caractère personnel n'en serait alors que plus cohérente et permettrait ainsi de garantir une sécurité juridique plus large en ce domaine [475]. Cette évolution viendrait également renforcer l'objectif de protection des données à caractère personnel. En effet,

[471] V. Cass. crim., 13 janv. 2009, *SACEM et autres c/ Cyrille Y.*, pourvoi n° 08-84.088, *D.* 2009, AJ, p. 497, obs. J. Daleau ; *Dr. pénal* mai 2009, Étude 10, p. 5 et s., note L. Flamant ; *RTD com.* 2010, p. 310 et s., note F. Pollaud-Dulian ; *Comm. com. électr.* avril 2009, comm. 31, p. 25 et s., note C. Caron (« *les constatations visuelles effectuées* […] *par un agent assermenté qui, sans recourir à un traitement préalable de surveillance automatisé, utilise un appareillage informatique et un logiciel de pair à pair, pour accéder manuellement, aux fins de téléchargement, à la liste des œuvres protégées irrégulièrement proposées sur la toile par un internaute, dont il se contente de relever l'adresse IP pour pouvoir localiser son fournisseur d'accès en vue de la découverte ultérieure de l'auteur des contrefaçons, rentrent dans les pouvoirs conférés à cet agent par la disposition précitée, et ne constituent par un traitement de données à caractère personnel relatives à ces infractions, au sens* […] *de la loi* [Informatique fichiers et libertés] »). – Commentant cet arrêt, Christophe CARON souligne le caractère ambigu de la décision : « *Si l'on en croit la Cour de cassation, on a le sentiment que, au stade de sa collecte par l'agent assermenté, l'adresse IP ne semble pas répondre à la qualification de donnée personnelle* » (note sous Cass. crim., 13 janv. 2009, arrêt préc., *Comm. com. électr.* avril 2009, comm. 31, p. 25 et s.)). – V. dans le même sens, Cass. crim., 15 juin 2009, pourvoi n° 08-88560, *RLDI* sept. 2009, n° 1507, p. 16 et s., note L. Costes et M. Trézéguet.

[472] En faveur de la qualification de données à caractère personnel, v. not. Jean FRAYSSINET, « La traçabilité des personnes sur l'internet, une possible menace pour les droits et libertés », *in Traçabilité et responsabilité*, art. préc., spéc. n°s 10-11, pp. 94-95 (*in* Philippe PEDROT (sous la dir.), *Traçabilité et responsabilité*, Economica, 2003). – Lionel COSTES et Jean-Baptiste AUROUX qui sont favorables à l'approche du TGI de St Brieuc (v. obs. sous TGI Saint-Brieuc, 6 sept. 2007, jugement préc., *RLDI* oct. 2007, n° 1028, p. 26 et s.). –*Contra* Frédéric LECOMTE et Marie-Hélène LEMAITRE qui, saluant la solution dégagée par les deux arrêts de la cour d'appel de Paris de 2007 précités, rejettent la qualification systématique de l'adresse IP en tant que donnée à caractère personnel, en raison notamment de l'attribution dynamique d'adresses IP par les FAI (« Inconnue juridique à cette adresse (IP) ou les affres du débat autour de la qualification de donnée à caractère personnel de l'adresse IP », *Expertises* 2008, p. 174 et s.). – Les incertitudes que suscite l'adresse IP conduisent même certains à proposer une nouvelle catégorie spécialement créée pour ce type de donnée, à savoir celle de « *donnée potentiellement nominative* », catégorie dans laquelle viendraient s'ajouter les numéros de ligne téléphoniques fixes ou les numéros d'immatriculation de véhicules (Fabrice MATTATIA, « Internet face à la loi Informatiques et libertés : l'adresse IP est-elle une donnée à caractère personnel ? », *Gaz. Pal.* 15 janv. 2008, p. 9 et s.).

[473] Sur l'importance d'une intervention législative destinée à mettre fin à cette controverse (v. par ex. Florence CHAFIOL-CHAUMONT et Antoine BONNIER, « L'identification des " pirates du Web " à partir de leur adresse IP », *RLDI* mai 2009, n° 1625, p. 84 et s. – Laurent SUZSKIN et Maxime DE GUILLENCHMIDT, « La qualification de l'adresse IP au centre de la lutte contre le téléchargement illicite sur les réseaux « peer to peer », *RLDI* déc. 2007, n° 1095, p. 6 et s. – Romain PERRAY, « Adresse IP et données personnelles : un besoin de convergence d'interprétations entre juges, *Gaz. Pal.* 30 avr. 2009, p. 6 et s.).

[474] V. en ce sens, Yves DETRAIGNE et Anne-Marie ESCOFFIER suggérant ainsi de modifier l'article 2 de la loi IFL en ajoutant la disposition suivante : « *Constitue en particulier une donnée à caractère personnel toute adresse ou tout numéro identifiant l'équipement terminal de connexion à un réseau de communication* » (art. 2 de la proposition de loi visant à mieux garantir le droit à la vie privée à l'heure du numérique, Doc. Sénat n° 93, enregistrée le 6 novembre 2009, disponible sur : http://www.senat.fr/leg/ppl09-093.pdf). – Sur cette proposition, v. not. Olivier PROUST, « État des lieux sur la proposition de loi du Sénat visant à modifier la loi " Informatique et libertés " », *RLDI* déc. 2009, n° 1823, p. 39 et s.

[475] À ce titre, le G29, à propos de l'adresse IP, a considéré que « *à moins que les fournisseurs d'accès internet soient en mesure de déterminer avec une certitude absolue que les données personnelles correspondent à des utilisateurs non identifiables, par mesure de sécurité, ils devront traiter toutes les informations IP comme des données à caractère personnel* » (Avis n° 4/2007 sur le concept de données à caractère personnel, avis spéc., spéc. pp. 18-19).

faute d'un régime encadrant la collecte de ce type de données, leurs titulaires ne bénéficieraient dès lors d'aucun fondement juridique pour se protéger contre des collectes abusives.

B. LES TRAITEMENTS DE DONNEES OPERES PAR LES « SPAMMEURS »

188. L'acception large de la notion de traitement. L'article 2, alinéa 3 de la loi IFL définit le traitement comme « *toute opération ou tout ensemble d'opérations portant sur de telles données, quel que soit le procédé utilisé, et notamment la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction* ». La loi de 2004 a ainsi vocation à s'appliquer dès lors que des données à caractère personnel font l'objet d'un traitement [476], que ce dernier soit automatisé [477] ou non [478].

189. Les opérations réalisées par les « spammeurs » : des traitements. Au regard de la définition adoptée par le législateur français, la collecte d'adresses électroniques réalisée par les « spammeurs » est, sans conteste, incluse dans cette notion de même que toute utilisation ultérieure qui consisterait à les enregistrer, les conserver ou encore à les utiliser à des fins d'envois. Toutefois, en l'absence de définition précise de la notion de collecte, la question se pose de savoir si celle-ci est subordonnée à l'enregistrement des

[476] Pour une critique de la notion de « traitement » visée par la loi IFL, v. Julien LE CLAINCHE, *L'adaptation du droit des données à caractère personnel aux communications électroniques,* thèse sous la dir. de Nathalie MALLET-POUJOL et Jean FRAYSSINET, Montpellier 1, 2008, spéc. n° 137 et s., p. 180 et s.

[477] La loi de 1978, en son article 5, en accord avec l'article 2 de la Convention de l'Europe et l'interprétation de la CNIL, avait déjà adopté une conception large de cette notion permettant ainsi une « *adaptation à l'évolution rapide des services et des outils informatiques* », pour reprendre les mots de Jean FRAYSSINET. Il précise à cet égard que « *le concept de traitement automatisé entendu largement impose de dépasser l'idée selon laquelle l'usage d'un ordinateur (conçu au sens commun du terme) gérant un fichier est seulement à envisager* ». Entrent, par exemple, dans cette catégorie la messagerie électronique, l'usage d'une machine à des fins d'adressage automatique nominatif (*mailing*), etc. (*Informatique fichiers et Libertés, op. cit.,* spéc. n^{os} 87-91, p. 36 s.).

[478] Contrairement à la loi de 1978 qui restait silencieuse sur la notion de « fichier non automatisé », l'alinéa 1er de l'article 2 de la loi de 2004 précise que la loi concerne également les traitements non automatisés de données à caractère personnel, c'est-à-dire les traitements manuels, à condition que ces derniers soient organisés en fichiers. À cet égard, l'alinéa 4 de l'article 2 de la loi de 2004 définit un fichier de données à caractère personnel comme « *tout ensemble structuré et stable de données à caractère personnel accessibles selon des critères déterminés* » (annuaires, répertoires papier, comptes rendus de réunion classés par date ou par nom, etc.). – Sur la notion de « fichier non automatisé » avant la loi de 2004, v. not. Jean FRAYSSINET, *Informatique fichiers et Libertés, op. cit.*, spéc. n^{os} 92-100, pp. 38-40.

données [479]. Telle est la question à laquelle la jurisprudence française a dû répondre dans une espèce où un « spammeur » utilisait un logiciel qui avait pour caractéristique de ne pas conserver en mémoire l'adresse électronique collectée et de procéder à l'envoi de messages dès sa captation.

190. Contexte et faits de l'espèce. Dans le prolongement de son rapport intitulé *Le publipostage électronique et la protection des données personnelles* [480], la CNIL avait lancé l'« opération boîte à *spam* » [481] au cours de laquelle elle avait créé une adresse électronique <spam@cnil.fr> permettant aux internautes d'y adresser les messages qu'ils estimaient être des *spams*. Après l'examen de centaines de milliers d'*e-mails* non sollicités que la CNIL avait reçus sur l'adresse qu'elle avait spécialement créée à cet effet, la Commission fut conduite à dénoncer au Parquet cinq sociétés les plus régulièrement citées par les internautes [482]. Parmi ces dernières, la Commission avait constaté la réception de plus de six cent cinquante *spams* émanant de la société ALLIANCE BUREAUTIQUE SERVICE (ABS) moins de trois mois après l'ouverture de cette boîte. Il lui était reproché d'utiliser et de proposer à la vente deux logiciels permettant à ses utilisateurs de capturer des adresses électroniques dans les espaces publics (forums de discussions, sites *Web*, annuaires, etc.) sans le consentement préalable des personnes concernées : l'un dénommé « Robot Mail » qui permettait de collecter et d'enregistrer ces adresses qu'il conservait dans un fichier afin de les utiliser ultérieurement, l'autre appelé « Freeprospect » qui permettait de collecter les données mais sans les enregistrer.

191. Problématique. Pour le premier robot, aucune difficulté ne s'était posée : la collecte avait bien eu lieu et les données étaient stockées dans les bases de données. En revanche, le second logiciel suscitait davantage d'interrogations. La question qui se posait aux magistrats était celle de savoir si le simple envoi de messages publicitaires à des adresses qui n'avaient pas été enregistrées, caractérisait une collecte au sens de la loi.

---

[479] À cet égard, Jean FRAYSSINET faisait remarquer que « *la collecte – terme non défini mais* [qui constitue] *généralement la première étape du processus de traitement de données* » (*Atteintes aux droits de la personne résultant des fichiers ou des traitements informatiques, J.-Cl. Pénal Code, Art. 226-16 à 226-24*, Fasc. 20, 2005, spéc. n° 263).

[480] Rapport préc.

[481] CNIL, délibération n° 02-074 du 24 octobre 2002 portant adoption du rapport relatif à l'opération « Boîte à *spams* » *in Rapport d'activité 2002*, n° 23, Doc. fr., 2003, spéc. p. 224. – Cécile ALVERGNAT (Rapport CNIL présenté par), *Opération " Boîte à spams " : Les enseignements et les actions de la CNIL en matière de communications électroniques non sollicitées*, 24 octobre 2002, rapport préc., spéc. p. 16 et s.

[482] CNIL, délibérations n° 02-075 (concernant la Société ABS), n° 02-076 du 24 oct. 2002 (concernant la Société BV COMMUNICATION), n° 02-077 (concernant la Société GREAT-MEDS.COM), n° 02-078 (concernant la Société SUNILES), n° 02-079 (concernant une lettre le Top 50 des sites X) du 24 octobre 2002 portant dénonciation au Parquet d'infractions à la loi du 6 janvier 1978, *in Rapport d'activité 2002*, rapport préc., spéc. p. 225 et s.

192. Une définition désormais étendue de la collecte. Pour sa défense, la société ABS avait soutenu avec succès en première instance que l'absence de capture et d'enregistrement des données nominatives écartait la qualification de collecte, le logiciel « Freeprospect » se cantonnant à cibler directement l'adresse électronique concernée à laquelle était transmis instantanément l'*e-mail* publicitaire [483]. Écartant cet argument, la chambre criminelle de la Cour de cassation avait, dans un arrêt du 14 mars 2006, jugé que le logiciel « Freeprospect » réalisait bien une collecte de données nominatives, opération définie comme « *le fait d'identifier des adresses électroniques et de les utiliser, même sans les enregistrer dans un fichier, pour adresser à leurs titulaires des messages électroniques* » [484]. Par cet arrêt, la Cour de cassation abandonnait ainsi une définition restrictive de la notion de collecte : cette opération était désormais caractérisée par le simple fait d'identifier et d'utiliser des données nominatives en vue de leur traitement ultérieur, indépendamment de leur enregistrement dans un fichier. Cette solution est particulièrement opportune puisqu'elle permet d'une part, de se rapprocher de façon cohérente de la définition du « traitement » posée par l'article 2 de la loi de 2004 précité et d'autre part, d'anticiper les difficultés qui allaient inéluctablement se poser à l'avenir dans l'hypothèse des *Blue spams*. En effet, au regard des spécificités de captation des données *Bluetooth*, il existe de fortes chances pour que les « spammeurs » s'inspirent de la défense de la société ABS pour tenter d'échapper au respect de la loi IFL. En effet, la captation de ce type de données opère selon un mode original, similaire à celui décrit par la société ABS. L'activation de la fonction *Bluetooth* sur un téléphone mobile rend l'identifiant de l'utilisateur visible par toute personne également connectée au réseau *Bluetooth*. Dans cette hypothèse, le « spammeur » tentera de contester l'existence d'une collecte puisqu'il se limite à cibler les données, sans les capturer ni les enregistrer. En appliquant de façon systématique la solution dégagée de l'arrêt du 14 mars 2006, cela permettrait de prévenir les éventuels conflits d'interprétations qui pourraient

[483] TGI Paris, 17e ch., 7 déc. 2004, *Ministère public / Fabrice H.*, jugement préc. (rappelant que le fait de « [c]*ollecter des données signifie les recueillir et les rassembler, ce qui implique leur enregistrement ou leur conservation dans un fichier* », le tribunal constate qu' « [i]*l ne résulte d'aucun des éléments produits que les adresses collectées faisaient l'objet d'un stockage ou d'un enregistrement* »). – Sur l'interprétation restrictive de la notion de collecte adoptée par les juges du fond, v. Julien LE CLAINCHE, *L'adaptation du droit des données à caractère personnel aux communications électroniques*, thèse préc., spéc. n° 152, p. 196. – La Cour de Cassation avait également eu l'occasion de se prononcer en ce sens antérieurement, v. par exemple Cass. crim. 3 nov. 1987, pourvoi n° 87-83429, *Bull. crim.*, n° 382 (pour que le délit prévu à l'article 226-18 du Code pénal soit constitué, « *il faut non seulement que des données aient été collectées par des moyens frauduleux, déloyaux ou illicites* […] *mais encore que ces données soient enregistrées ou conservées dans un fichier* »).

[484] Cass. crim., 14 mars 2006, arrêt préc. – La cour d'appel, quant à elle, ne s'était pas risquée à répondre à cette question et avait esquivé le débat en relevant seulement que logiciel « Freeprospect » avait pour fonction à la fois de collecter des informations et de les traiter instantanément, et qu'il y avait eu nécessairement mémorisation de l'adresse concernée « *ne serait-ce qu'un instant infime sur la mémoire vive* » pour permettre l'envoi du message, la réunion de ces deux opérations permettant de sanctionner le « spammeur » sur le fondement de l'article 226-18 du Code pénal (CA Paris, 11e ch., sect. B, 18 mai 2005, *Fabrice H. c/ Ministère public, inédit*). – Sur cette disposition, v. *infra* : n° 243.

se poser au regard des circonstances particulières dans lesquelles ces données *Bluetooth* sont captées.

§ 2. LE *SPAMMING*, UNE PRATIQUE EN VIOLATION DE LA LOI INFORMATIQUE, FICHIERS ET LIBERTES

193. En procédant à des traitements au sens de la loi IFL [485], le « spammeur » endosse automatiquement la qualité de responsable de traitement, c'est-à-dire celui « *qui détermine ses finalités et ses moyens* » [486] et par conséquent, est tenu au respect de l'ensemble des dispositions de la loi IFL [487]. Bien que la loi informatique, fichiers et libertés ait pleinement vocation à réglementer la pratique du *spamming*, nous verrons qu'elle se trouve malmenée par le « spammeur », tant au regard des obligations transgressées par ce dernier (A.) que des droits des titulaires qu'il ignore totalement (B.).

A. DES OBLIGATIONS LEGALES TRANSGRESSEES PAR LES « SPAMMEURS »

194. Dans cette perspective de protection des données à caractère personnel, toute opération de collecte et de traitement doit être réalisée dans le respect des principes directeurs qui gouvernent leur mise en œuvre, principes dont les premiers jalons avaient déjà été posés par la directive de 1995 et la loi de 1978 [488]. Afin de satisfaire ces principes, la loi de 2004 a imposé au responsable de traitement un certain nombre d'obligations lorsqu'il procède à la collecte et à l'exploitation de données nominatives [489], obligations auxquelles le « spammeur » doit se conformer en cette qualité (2.). Toutefois, la confrontation du *modus operandi* [490] du « spammeur » à la loi IFL démontrera que ce dernier contrevient aux

[485] V. *supra* : n° 189.
[486] Art. 3-I. loi n° 2004-801 : « *Le responsable d'un traitement de données à caractère personnel est, sauf désignation expresse par les dispositions législatives ou réglementaires relatives à ce traitement, la personne, l'autorité publique, le service ou l'organisme qui détermine ses finalités et ses moyens* ».
[487] Pour une étude détaillée sur la qualité de responsable d'un traitement, v. not. G29, Avis n° 1/2010 sur les notions de « responsable du traitement » et de « sous-traitant », 16 février 2010, 00264/10/Fr, Wp 169, disponible sur : http://www.cnpd.public.lu/fr/publications/groupe-art29/wp169_fr.pdf.
[488] À l'issue d'une analyse comparative du texte de 2004 et de sa version antérieure, le professeur Jean FRAYSSINET a souligné que « *la tendance est nettement à la continuité pour les principes de base, et même pour leur organisation et leur mise en œuvre. Il y a évolution et non révolution* », les modifications procédant davantage d'un « *ajustement* » de la loi pour s'aligner sur la directive 95/46/CE (« La loi relative à l'Informatique, aux fichiers et aux libertés, modifiée par la loi du 6 août 2004 : continuité et/ou rupture ? », chron. préc., spéc. p. 55).
[489] Sur l'importance de la sensibilisation des entreprises à la culture « informatique et libertés » et notamment quant aux obligations qui leur incombent en qualité de responsable de traitement, v. not. Fabrice NATALSKI, « La loi " Informatique et libertés " n'est plus l'éternelle arlésienne », *RLDI* janv. 2008, n° 1158, p. 74 et s.
[490] V. *supra :* n° 90 et s.

principes directeurs fixés par la loi (1.) et *a fortiori*, aux différentes obligations qui lui incombent.

1. Le non-respect des principes directeurs gouvernant la collecte et les traitements de données

195. Tout responsable de traitement est tenu au respect des principes de légitimité (a.), de loyauté (b.), de finalité (c.), de proportionnalité et de pertinence (d.) lorsqu'il entreprend de collecter et de traiter des données nominatives, principes auxquels se soustrait clairement le « spammeur ». L'étude de ces principes sera également l'occasion de s'interroger sur leur mise en œuvre dans le cas particulier des *Blue spams* qui, nous le verrons, pose en pratique des questions particulières.

a. Le principe de légitimité

196. Le recueil du consentement préalable. Aux termes de l'article 7 de la loi n° 2004-801, un traitement de données à caractère personnel ne peut, par principe, être opéré que si le responsable du traitement a « *reçu le consentement de la personne concernée* » [491]. La loi impose donc à la charge du responsable du traitement une obligation générale de prouver que la personne dont les données font l'objet d'un traitement a exprimé son consentement préalable (système dit de l'*opt-in* [492]) [493]. Il convient également de préciser qu'une collecte d'adresses électroniques, même réalisée dans le respect de l'ensemble des prescriptions légales, et notamment en recueillant le consentement préalable de la personne concernée, n'autorise pas, par la suite, à les vendre ou les céder à des tiers sans le consentement préalable de la personne concernée, cette dernière ayant toujours la possibilité

[491] Rappr. de l'article 22 de la loi pour la confiance dans l'économie numérique qui subordonne les envois commerciaux au consentement préalable des destinataires (sur ce point, v. *infra* : n° 295 et s.). – V. ég. Cass. crim. 14 mars 2006, arrêt préc.

[492] Sur les systèmes d'*opt-in* et d'*opt-out*, v. *infra :* n[os] 284-288

[493] À moins que ce dernier ne parvienne à démontrer le consentement positif de la personne concernée ou d'en justifier par l'une des dérogations prévue à l'alinéa 2 de l'article 7 de la loi de 2004 et notamment : « [l]*e respect d'une obligation légale incombant au responsable du traitement* […] *5° La réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le destinataire, sous réserve de ne pas méconnaître l'intérêt ou les droits et libertés fondamentaux de la personne concernée* ». – V. CNIL, Document d'orientation « pour la mise en œuvre de dispositifs d'alerte professionnelle conformes à la loi du 6 janvier 1978 modifiée en août 2004, relative à l'informatique, aux fichiers et aux libertés », 10 novembre 2005, disponible sur : http://www.cnil.fr/fileadmin/documents/La_CNIL/actualite/CNIL-docori-10112005.pdf (qui analyse la conformité de dispositifs d'alerte professionnelle (« *whistleblowing* ») avec les exceptions légales de l'article 7 de la loi de 2004).

de s'opposer à ce que ses données soient transférées à des tiers (*opt-out*) [494]. Le respect de ce principe est donc primordial puisqu'il conditionne la mise en œuvre des droits reconnus aux titulaires des données et notamment l'exercice de son droit d'opposition [495].

197. *Quid* du *spamming ?* Comme nous l'avons expliqué précédemment, la collecte d'adresses électroniques est réalisée le plus souvent au moyen de logiciels capables d'aspirer toutes les adresses figurant dans les espaces publics de l'internet [496]. Réalisé à l'insu des personnes concernées [497], ce mode de collecte apparaît incontestablement incompatible avec l'obligation d'obtenir le consentement préalable de la personne concernée. L'apparition des *Blue spams* a également suscité de nouvelles difficultés. Si les données traitées par *Bluetooth* venaient à être considérées officiellement comme des données à caractère personnel, la loi IFL aurait vocation à s'appliquer. Cette hypothèse conduit à s'interroger quant aux modalités de recueil du consentement préalable du titulaire de ces données. Dans ce cas de figure précis, dès l'instant où la personne a activé sur son téléphone mobile la fonction *Bluetooth*, son identifiant *Bluetooth* est visible par toute autre personne connectée au réseau *Bluetooth*. Pour échanger des données entre deux terminaux connectés au réseau *Bluetooth*, ces derniers doivent être appairés, ce jumelage étant soumis à la confirmation d'un mot de passe commun. Dès l'instant où la vérification est validée, les personnes acceptent d'entrer en contact, ce qui vaut consentement à utiliser ses identifiants pour recevoir des messages. Cette autorisation peut toutefois être retirée à tout moment en envoyant par exemple un message indiquant le mot « Stop » ou en désinscrivant son mobile, ce qui implique pour les annonceurs d'établir et de maintenir à jour une liste contenant les demandes d'opposition.

b. Le principe de loyauté

198. Définition. Aux termes de l'article de l'article 6-1° de la loi du 6 août 2004, la collecte et le traitement des données doivent être « *loyaux et licites* » [498]. Cette obligation de

[494] La CNIL rappelait ainsi que « *La cession de ce fichier de mails est régulière au regard des règles de protection des données personnelles dès lors que le site qui a initialement collecté les adresses et s'apprête à les céder à un tiers, a informé les personnes concernées que leurs données pouvaient être communiquées à un tiers à des fins de prospection* » (*Le publipostage électronique et la protection des données personnelles*, rapport préc., spéc. p. 19).
[495] Sur le droit d'opposition, v. *infra* : n° 224.
[496] Sur ce mode de collecte, v. *supra* : n^{os} 59 et 92.
[497] V. not. Cass. crim., 14 mars 2006, arrêt préc.
[498] L'article 6.1. (a) dir. 95/46/CE prévoyait que les données devaient être « *traitées loyalement et licitement* », cette disposition faisait écho à l'article 25 de la loi de 1978 qui interdisait « *la collecte de données opérée par tout moyen frauduleux, déloyal ou illicite* ». – La loyauté occupe une place centrale dans le droit positif français :

transparence sous-tend une obligation pour tout responsable de traitement d'informer la personne de la finalité poursuivie par le(s) traitement(s), des destinataires des données mais aussi de son droit d'opposition, d'accès et de rectification. Le principe de loyauté entretient ainsi un lien étroit avec différents droits et obligations fixés par la loi [499].

199. Le cas particulier des messages *via Bluetooth*. Le principe de transparence impose de fournir à l'utilisateur diverses informations lors de la collecte. La question se pose de savoir en pratique comment cette information peut être transmise à la personne concernée en cas d'envois de messages *via Bluetooth*. Plusieurs modes peuvent être envisagés : on peut penser, par exemple, à l'affichage à proximité des bornes *Bluetooth* ou sur une page *Web* spécifiquement créée à cet effet.

200. La question de l'aspiration des adresses circulant sur l'internet. Classiquement, la collecte d'adresses électroniques est réalisée dans les espaces publics de l'internet au moyen de robots capables d'aspirer automatiquement sur leur passage toutes ces données à l'insu des personnes concernées et permet ainsi de construire d'immenses bases de données de prospects à un coût dérisoire. Toutefois, l'absence de précision quant à la notion de loyauté [500] ne permet pas de trancher clairement la question de savoir si ce type de collecte est considéré comme déloyal [501]. La jurisprudence a permis d'apporter des précisions sur ce point à l'occasion de l'affaire précitée impliquant la société ABS [502]. La CNIL qui avait dénoncée cette dernière considérait que les collectes qu'elle avait réalisées étaient illégales et

---

en droit civil, en vertu de l'article 1116 du Code civil, le dol qui est un défaut de loyauté, est sanctionné par la nullité du contrat, de même, l'article 1134 du Code civil impose d'exécuter les conventions de bonne foi constitue une autre manifestation de la loyauté. On peut également retrouver cette exigence à l'article L. 212-1 du Code de la consommation qui punit la falsification et les fraudes de peines d'emprisonnement et d'une amende ou encore à l'article L. 121-1 du même code qui fait de la loyauté du professionnel une exigence gouvernant l'ensemble des pratiques commerciales. En effet, ce principe s'impose de façon générale pour tous les messages publicitaires : la publicité trompeuse est ainsi prohibée (article L.121-1 C. conso) et le principe de loyauté doit être respecté en matière de publicité comparative (article L. 121-8 et s. C. conso) (v. not. Guy RAYMOND, *Publicité : Règles générales, J.- Cl. Commercial*, Fasc. 930, 2002).

[499] Sur ces droits et obligations, v. *infra* : n° 162 et s. et 223 et s.

[500] V. en ce sens, André LUCAS, Jean DEVEZE et Jean FRAYSSINET soulignant que : « *si le concept de licéité ne soulève pas d'interrogations, il n'en est pas de même pour celui de loyauté, riche de sens mais flou, impliquant une appréciation morale ou éthique autant que juridique, intégrant fortement les faits contextuels* » (*Droit de l'informatique et de l'internet*, *op. cit.*, spéc. n° 201, p. 126). – De même à l'occasion de l'étude de l'article 226-18 du Code pénal qui sanctionne le caractère déloyal des traitements, Jean FRAYSSINET faisait remarquer que le terme « déloyal » auquel fait référence cette disposition n'a pas un sens déterminé dans le vocabulaire juridique mais revêt un « *sens plus impressionniste qui amènera à considérer les comportements, les intentions, les faits contextuels, en laissant une marge d'appréciation au juge* » (*Atteintes aux droits de la personne résultant des fichiers ou des traitements informatiques*, fasc. préc., spéc. n° 265).

[501] Déjà en ce sens, Pierre LECLERCQ observait que « *cette exigence* [de loyauté], *posée en termes généraux, laisse ouvert un certain nombre de questions. Ainsi, celle de savoir s'il est loyal ou déloyal de collecter des données dans les espaces publics de l'Internet, par exemple les forums de discussion, à l'insu des personnes concernées* » (« La CNIL, garante de la finalité, de la loyauté et de la sécurité des données personnelles » *in* Marie-Christine PIATTI, *Les libertés individuelles à l'épreuve des NTIC*, *op. cit*., spéc. p. 114).

[502] Sur les circonstances de cette affaire, v. *supra* : n° 190.

déloyales [503]. Dans un premier temps, par un jugement en date du 7 décembre 2004, le tribunal de grande instance de Paris avait relaxé le dirigeant de la société « spammeuse » au motif que « [c]*ompte-tenu de l'accessibilité universelle de l'internet, un tel recueil* […] *de données disponibles sur les espaces publics* », n'étant interdit par aucune disposition expresse et n'impliquant l'usage d'aucun procédé frauduleux, ne pouvait ainsi être considéré comme déloyal du seul fait que les intéressés n'aient pas été informés [504]. Le Parquet a fait appel de cette décision à la demande de la CNIL. Infirmant ce jugement, la cour d'appel de Paris, dans un arrêt du 18 mai 2005, a condamné le « spammeur » en considérant que la collecte, assurée au moyen du logiciel « Robot Mail », avait été réalisée par un moyen illicite et déloyal. Pour fonder sa décision, la cour d'appel avait relevé que les adresses collectées dans les espaces publics avaient « *donné lieu à une utilisation sans rapport avec l'objet de leur mise en ligne* » [505] et avait rappelé que tout traitement de données à caractère personnel devait être opéré après avoir recueilli le consentement de la personne concernée. Or, en l'espèce, cette dernière exigence faisait défaut et ce, malgré l'existence d'un droit d'opposition, droit qui supposait que la personne soit informée des traitements envisagés sur ses données. Entérinant ainsi la position soutenue en 2002 par la CNIL, la cour d'appel condamnait le « spammeur » en considérant que la collecte de données nominatives à l'insu des personnes concernées était contraire à la législation relative à la protection des données [506]. Cette décision fut par la suite confirmée par la chambre criminelle de la Cour de cassation dans l'arrêt du 14 mars 2006 précité et qui avait jugé comme déloyal, « *le fait de recueillir, à leur insu, des adresses électroniques personnelles de personnes physiques sur l'espace public d'internet, ce procédé faisant obstacle à leur droit d'opposition* » [507]. Le caractère déloyal découlait donc des conditions dans lesquelles était opérée la collecte. De cette façon, la chambre criminelle affirme clairement que les données nominatives qui circulent sur le réseau ne sont pas de libre parcours et que leur utilisation reste soumise au respect des exigences posées par la loi. Toute aspiration des données dans les espaces publics est, par définition, réalisée à l'insu des personnes concernées et prive alors ces dernières

[503] CNIL, délibération n° 02-075, préc., *in Rapport d'activité 2002*, spéc. p. 226.
[504] TGI Paris, 17e ch., 7 déc. 2004, *Fabrice H. c/ Ministère public*, jugement préc.
[505] Art. 226-21 C. pén. (incriminant le détournement de finalité telle que définie notamment par une déclaration préalable au traitement envisagé).
[506] CA Paris, 11e ch., sect. B, 18 mai 2005, arrêt préc. – CNIL, *Rapport d'activité 2005*, n° 26, Doc. fr., 2006, spéc. p. 71.
[507] Cass. crim., 14 mars 2006, arrêt préc. – *Contra* Cass. crim., 25 oct. 1995, pourvoi n° 94-85.781 ; *Bull. crim.* 1995, n° 320 (selon la Cour de cassation, « *la loi du 6 janvier 1978 ne fait nulle obligation au responsable du fichier, qui recueille auprès de tiers des informations nominatives aux fins de traitement, d'en avertir la personne concernée* ». Est ainsi cassé l'arrêt qui avait condamné le responsable d'un fichier pour non-respect du droit d'opposition au motif que « *la mise en oeuvre* […] *du droit d'opposition* […] *suppose que* [la personne concernée] *soit avisée, préalablement à son inscription sur un fichier, de ce que des informations nominatives la concernant sont susceptibles de faire l'objet d'un traitement* »). – V. Pierre LECLERCQ, « Un an d'application de la législation " informatique et libertés ", *Comm. com. électr.* juin 2006, chron. 6, p. 17 et s., spéc. n° 10 ; *Comm. com. électr.* oct. 2007, chron. 9, p. 27 et s., spéc. n° 11.

d'exercer leur droit d'opposition, ce dernier ne pouvant être mis en œuvre sans avoir été informé des collectes réalisées. On constate ici un enchevêtrement des principes : la violation du droit d'opposition résultant du non-respect du principe de légitimité [508].

c. Le principe de finalité

201. Définition. Le principe de finalité est consacré comme un principe central et directeur du dispositif de la loi IFL. Transposant fidèlement la directive 95/46/CE [509], l'article 6-2° de la loi de 2004 [510] impose que « *les données* [soient] *collectées pour des finalités déterminées, explicites et légitimes et ne* [soient] *pas traitées ultérieurement de manière incompatible avec ces finalités* », marquant ainsi un progrès par rapport à l'ancienne loi qui restait silencieuse sur ce point [511]. En vertu de ce principe, toute cession, location de fichiers, notamment d'adresses, ou échange de données nominatives pour des finalités autres que celles initialement prévues est prohibée. L'article 6 ajoute les données doivent être non seulement « *adéquates, pertinentes et non excessives* » [512] mais aussi « *exactes, complètes et, si nécessaire, mises à jour* » [513] au regard des finalités pour lesquelles elles sont collectées et traitées. Enfin, cette même disposition précise que les données doivent être conservées pendant une durée qui doit être limitée à celle nécessaire pour répondre à ces finalités [514].

[508] En effet, l'article 226-18 du Code pénal qui incrimine toute collecte frauduleuse, déloyale et illicite, et sur lequel se fonde la Cour de cassation, côtoie l'article 226-18-1 du même code qui incrimine « *le fait de procéder à un traitement de données à caractère personnel concernant une personne physique malgré l'opposition de cette personne, lorsque ce traitement répond à des fins de prospection, notamment commerciale, ou lorsque cette opposition est fondée sur des motifs légitimes* » ainsi que l'article 226-21 du Code pénal qui incrimine le détournement de finalité (sur ces dispositions pénales, v. *infra* : n° 195 et s.). – Sur cet enchevêtrement des dispositions, v. Jean FRAYSSINET qui constate que « *les actes visés à l'article 226-18 peuvent recouper d'autres infractions* » (*Atteintes aux droits de la personne résultant des fichiers ou des traitements informatiques*, fasc. préc., spéc. n° 268).

[509] Art. 6 b) dir. 95/46/CE.

[510] Ce qui marque une évolution par rapport à la loi de 1978 dans laquelle ce principe n'apparaissait qu'en filigrane.

[511] À cet égard, Jean FRAYSSINET salue cette évolution « *tant le principe de finalité est essentiel à la compréhension et à la pratique de la loi* » (« La loi relative à l'Informatique, aux fichiers et aux libertés, modifiée par la loi du 6 août 2004 : continuité et/ou rupture ? », chron. préc., spéc. p. 51).

[512] Art. 6-3° loi n° 2004-801.

[513] Art. 6-4° loi n° 2004-801.

[514] Art. 6-5° loi n° 2004-801. – Ce principe de finalité existe également en droit des biens et rejoint la question du patrimoine d'affectation qui consiste en l'affectation de certains biens à une finalité précise. La fiducie en est un exemple. La fiducie est définie comme « *l'opération par laquelle un ou plusieurs constituants transfèrent des biens, des droits ou des sûretés, ou un ensemble de biens, de droits ou de sûretés, présents ou futurs, à un ou plusieurs fiduciaires qui, les tenant séparés de leur patrimoine propre, agissent dans un but déterminé au profit d'un ou plusieurs bénéficiaires* » (art. 2011 C. civil). – Sur cette opération, v. not. Jean-Louis BERGEL, Marc BRUSCHI et Sylvie CIMAMONTI, *Traité de droit civil : Les biens*, (sous la dir. Jacques GHESTIN), 2e éd., L.G.D.J., 2010, spéc. n° 5 et s., 5 et s. – Gauthier BLANHUET et Jean-Pierre LE GALL, « La fiducie, une œuvre inachevée. Un appel à une réforme après la loi du 19 février 2007 », *JCP* 2007, éd. G., I. 169. – Phillippe DUPICHOT, « Opération fiducie sur le sol français », *JCP* 2007, éd. G., actu. 121.

202. Les fonctions du principe de finalité. L'article 6 de la loi de 2004 permet de dégager trois rôles assumés par ce principe. Le premier consiste à déterminer l'objet du traitement et en ce sens, acquiert une valeur informative. Le second se présente comme la justification du traitement dans la mesure où ce dernier ne peut être envisagé sans objectif. Selon Pierre-Alain WEILL, secrétaire général de la CNIL, « *la finalité représente l'objet d'un traitement automatisé tel que déclaré à la CNIL, qui justifie la création et l'existence d'un fichier nominatif* » [515]. Le principe de finalité a ainsi vocation à légitimer le traitement poursuivi. Enfin, il sert à délimiter le champ du traitement considéré [516] puisqu'il permet de sélectionner des données éligibles à un traitement légal. Ainsi, la collecte de données sera considérée comme légitime si elle répond à la finalité déclarée. À la suite de cette collecte, la finalité est destinée à contrôler la conformité de l'utilisation de ces données à la finalité déclarée et enfin de s'assurer que la durée de conservation des données n'est pas excessive au regard de l'objectif visé [517]. Innervant ainsi l'ensemble du processus de traitement des données, c'est-à-dire de leur collecte jusqu'à leur conservation en passant par l'ensemble des utilisations qui pourront en seront faites, ce principe peut être défini comme « *la colonne vertébrale de la loi du 6 janvier 1978* » [518].

203. *Quid* du *spamming ?* La confrontation de ce principe avec les pratiques utilisées par les « spammeurs » conduit une fois encore à conclure à la violation de la loi IFL. Tel est le cas par exemple lorsque le « spammeur » aspire des adresses électroniques figurant sur les forums de discussion à des fins de prospection commerciale alors même que ces données avaient initialement vocation à être utilisées aux seules fins de communication entre les membres dudit forum. De façon plus générale, la violation du principe de finalité intervient à l'occasion de toute collecte de donnés divulguées par l'internaute lors d'une inscription à un site *Web*, à une liste de diffusion ou à l'occasion d'un achat en ligne [519].

d. Les principes de pertinence et de proportionnalité, corollaires du principe de finalité

[515] Pierre-Alain WEILL, « État de la législation et tendances de la jurisprudence relatives à la protection des données à caractère personnel en droit pénal français », art. préc., spéc. p. 662.
[516] Frédéric LESAULNIER, *L'information nominative*, thèse préc., spéc. n° 83, p. 113.
[517] Sur ces différents aspects, v. Herbert MAISL, « État de la législation française et tendances de la jurisprudence relatives à la protection des données personnelles », *RIDC* 1978-3, p. 571 et s.
[518] Jean FRAYSSINET, *Informatique, fichiers et libertés*, *op. cit.*, spéc. n° 172, spéc. p. 73.
[519] Ces risques de détournement de finalité des traitements ont très tôt été identifiés par la CNIL qui, quinze ans auparavant, rapportait que « [l]*a collecte et l'exploitation des "E-mail" à des fins commerciales constitue un problème essentiel lié au développement du commerce électronique sur Internet. En effet, des informations communiquées par l'utilisateur sur Internet, dans un cadre souvent non commercial, peuvent être détournées de leur destination initiale* » (*Rapport d'activité 1996*, n° 17, Doc. fr., 1997, spéc., p. 93).

204. Le simple constat du non-respect du principe de finalité conduira inéluctablement à conclure que ses corollaires, les principes de pertinence (i.) et de proportionnalité (ii.), sont également ignorés par les « spammeurs ». Toutefois, afin de saisir précisément dans quelle mesure le *spamming* contrevient à ces principes, il est intéressant de les disséquer successivement. Cette étude mènera enfin à constater que leur mise en œuvre est délicate (iii).

i. Le principe de pertinence

205. Identification. Alors que dans la loi n° 78-17 le principe de pertinence a été dégagé, non pas à partir de la lettre du texte mais de son interprétation [520], la Convention 108 du Conseil de l'Europe du 28 janvier 1981 a, par la suite, nettement contribué à son émergence en affirmant expressément son existence [521]. L'article 6 de la loi de 2004 prévoit de la même façon qu'un traitement ne peut porter que sur des données qui « *sont adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et de leurs traitements ultérieurs* » [522]. Le respect du principe de pertinence est ainsi apprécié à la lumière de la finalité poursuivie par le traitement et constitue à ce titre une émanation de cette dernière.

206. Lien avec le principe de légitimité. Le principe de pertinence entretient également une relation étroite avec celui de légitimité puisque seules les données pertinentes

[520] Par exemple, l'article 6 de la loi n° 78-17 dispose que la CNIL sera « *chargée de veiller au respect des dispositions de la présente loi, notamment* […] *en contrôlant les applications de l'informatique aux traitements des informations nominatives* ». – La Cour de cassation n'a pas reconnu pour le moment ce principe, v. Cass. civ. 1re, 20 nov. 1990, *Mme Monanges c/ Kern et a.*, pourvoi n° 89-12.580, *Bull. civ.* I, n° 256 ; *JCP* 1992, éd. G., II. 21908, note J. Ravanas ; *D.* 1991, chron., p. 176, spéc. n° 2, obs. A. Bénabant. – *Contra* par ex. CA Versailles, 14 sept. 1989, *Jamet, Tesson et autre c/ consorts Girard*, *Gaz. Pal.* 1990, somm., p. 123.

[521] Art. 5 c. Convention 108 : « *Les données à caractère personnel faisant l'objet d'un traitement automatisé sont* « *adéquates, pertinentes et non excessives par rapport aux finalités pour lesquelles elles sont enregistrées* ». L'article 6.1 c. de la directive 95/46/CE reprend en substance la même exigence en imposant que les données à caractère personnel soient « *adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et pour lesquelles elles sont traitées ultérieurement* ».

[522] Si le principe de pertinence est clairement affirmé comme destiné à déterminer les données pouvant légitimement faire l'objet d'un traitement, il a également vocation à s'appliquer lors du processus de conservation des données. L'article 6-5° prévoit en effet que les données à caractère personnel doivent être « *conservées sous une forme permettant l'identification des personnes concernées pendant une durée qui n'excède pas la durée nécessaire aux finalités pour lesquelles elles sont collectées et traitées* ». Il semble incontestable que *« la durée nécessaire aux finalités* » exige une durée de conservation des données pertinente, s'appréciant par rapport à la finalité du traitement. Autrement dit, la conservation des données ne sera considérée comme légitime que si elle est strictement limitée à une durée nécessaire pour répondre à la finalité du traitement.

pourront légitimement faire l'objet du traitement envisagé [523]. Il endosse ainsi le rôle de répartiteur entre toutes les données nominatives dans la mesure où seules celles ayant un lien direct avec la finalité du traitement pourront être légitimement traitées. Les notions « *adéquates* » et « *non excessives* » semblent, quant à elles, participer à préciser les contours du principe de proportionnalité, sans imposer aucune obligation supplémentaire à l'égard de la notion de pertinence.

ii. Le principe de proportionnalité, prolongement du principe de pertinence

207. Une fonction d'arbitrage. Le principe de proportionnalité est destiné à s'appliquer chaque fois qu'il s'agit d'arbitrer des intérêts divergents afin de parvenir à une situation d'équilibre et d'éviter toute mesure restreignant un droit fondamental [524].

208. Une identification en filigrane. Le principe de proportionnalité n'est pas expressément visé par la loi de 2004 mais apparaît de façon sous-jacente à travers l'article 6-3° qui impose que les données soient « *adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et leurs traitements ultérieurs* » [525]. Il sert à vérifier le respect du principe de pertinence au regard de la finalité et seuls les traitements considérés comme proportionnés à la finalité visée seront réputés licites. Le rapport étroit existant entre les principe de proportionnalité et de pertinence permet ainsi de rendre effectif le principe de finalité. En pratique, ce lien est si étroit que l'un et l'autre sont utilisés sans réelle distinction, ce qui risque parfois de poser des difficultés à l'occasion de leur mise en œuvre. En tout état de cause, le principe de proportionnalité prend tout son sens en matière de *spamming* dans la mesure où, comme évoqué précédemment, l'enjeu face à des intérêts opposés est justement de trouver un équilibre entre les intérêts économiques des

[523] C'est en ce sens que Frédéric LESAULNIER a pu écrire que le principe de pertinence « *se situe dans le prolongement du principe de légitimité* » (*L'information nominative*, thèse préc., spéc. n° 189).
[524] Frédéric LESAULNIER a, à ce titre, souligné que « *le principe de proportionnalité est un principe juridique opératoire chaque fois qu'il s'agit de déterminer la légitimité d'une atteinte aux droits des personnes* » (*id.* spéc., n° 198).
[525] Anticipant l'adoption de la loi de 2004, certains auteurs ont souligné que si les principes – adéquat, pertinent et non excessif –, déjà inscrits à l'article 6c de la directive de 1995, « *n'étaient pas explicites dans la loi de 78,* [ils étaient] *déjà appliqués par la CNIL et le juge ; ils montrent* [ainsi] *la montée attractive du principe de finalité et établissent une sorte de proportionnalité entre la qualité des données et la finalité de leur traitement* » (André LUCAS, Jean DEVEZE et Jean FRAYSSINET, *Droit de l'informatique et de l'internet*, *op. cit.*, spéc. n° 205, p. 127).

« spammeurs » et ceux des titulaires des données qui aspirent à une meilleure protection de leurs données [526].

iii. Une mise en œuvre délicate de ces deux principes

209. Difficultés d'appréciation. Si en théorie l'obligation d'opérer des traitements pertinents et proportionnels au regard du principe de finalité ne soulève pas de question d'interprétation particulière, la mise en œuvre de ces principes se révèle néanmoins plus problématique et ouvre inévitablement une brèche dans l'effectivité de la loi [527]. En particulier, les difficultés d'appréciation du principe de pertinence sont liées à une certaine subjectivité que ce dernier induit et dont l'imprécision peut nuire à son dynamisme [528]. Par ailleurs, les incertitudes sont loin d'être dissipées lorsque l'on tente de se référer à une notion proche, celle d'« *adéquation* », puisqu'elle est également caractérisée par une certaine instabilité, son intensité variant en fonction de la disproportion constatée [529]. La question qui se pose est alors celle de savoir comment appréhender de façon pragmatique ces notions de pertinence et de proportionnalité. La réponse est essentielle puisque ces dernières tendent à expliciter le principe de finalité dans son application concrète. Pour tenter d'évaluer le principe de proportionnalité, le professeur Martine BEHAR-TOUCHAIS propose deux acceptions possibles, une « *proportionnalité purement mathématique* » ou une

[526] Sur cette opposition, v. *supra* n° 145 et s.

[527] À cet égard, Daniel GUTMANN souligne que « [l]*a logique du principe de pertinence est une logique floue. C'est ce qui rend si difficile son application concrète. On ne peut en effet se voiler le fait que l'appréciation du rapport de pertinence entre l'information recherchée et la finalité poursuivie pose souvent de sérieuses difficultés. En conséquence, on comprend que pour échapper à toute incrimination, les créateurs de fichiers automatisés puissent avoir tendance à déclarer à la CNIL des finalités vagues et étendues leur laissant une certaine marge de manœuvre. C'est alors l'effectivité du principe de pertinence qui se trouve affectée* » (*Le sentiment d'identité – Étude de droit des personnes et de la famille* (préf. François TERRE), tome 327, L.G.D.J., coll. *Bibl. dr. privé*, 2000, spéc. n° 293, p. 253).

[528] En effet, « *l'appréciation du caractère adéquat, pertinent et non excessif des données est autant subjective qu'objective ce qui augmente l'imprécision et la difficulté d'application sans parler des contestations possibles* » (André LUCAS, Jean DEVEZE et Jean FRAYSSINET, *Droit de l'informatique et de l'Internet*, *op. cit.*, spéc. n° 205, p. 127). – V. ég. Daniel GUTMANN qui souligne la « [d]*ifficulté de cerner avec précision la notion de pertinence, indétermination fréquente des finalités, tels sont les obstacles qui risquent de mettre à mal le principe de pertinence lui-même* » (*op. cit.*, spéc. n° 293, p. 254).

[529] Nicolas MOLFESSIS explique que « [l']*exigence d'adéquation peut être plus ou moins contraignante, selon qu'est sanctionnée une disproportion manifeste, excessive … ou une simple disproportion* ». L'auteur ajoute que « *la proportionnalité est alors appréhendée de façon positive, lorsque la recherche est celle d'une équivalence parfaite entre les termes du rapport ; elle est saisie de façon négative lorsque le contrôle porte uniquement sur une certaine disproportion* » (« Le principe de proportionnalité et l'exécution du contrat », *LPA* 30 sept. 1998, n° 117, p. 21 et s., spéc. note (2), p. 21). – Cette difficulté d'interprétation transparaît notamment dans l'appréciation de la durée de conservation des données qui oscille en pratique dans une fourchette relativement large puisqu'elle dépend du traitement envisagé (v. en ce sens, Jean FRAYSSINET qui rappelle que : « *la CNIL, lors des déclarations de traitements par le biais des normes simplifiées, apprécie avec pragmatisme la durée de conservation à respecter au cas par cas, en fonction essentiellement de la finalité du traitement. Elle tente de concilier la protection des individus avec celle de la collectivité qui va dans le sens de la conservation, pour la recherche historique ou épidémiologique par exemple. Tout dépendra de l'argumentation du déclarant. La durée peut être courte ou sans limite* » (*Informatique, fichiers et libertés*, *op. cit.*, spéc. n° 175, p. 74.)

« *proportionnalité finalisée* » qui introduit l'idée de juste mesure [530]. Notre préférence se tournera vers la seconde proposition qui, accordant une certaine souplesse dans l'évaluation de ce principe, permettra d'aboutir à une situation plus équilibrée « *tant par rapport aux objectifs légitimes poursuivis par l'auteur de la mesure, que par rapport aux objectifs légaux ou jurisprudentiels que l'auteur de la mesure se devait de poursuivre* » [531].

2. Le non-respect des obligations en matière de collecte et de traitement

210. Tout responsable de traitement est tenu de respecter un certain nombre d'obligations dès l'instant où il envisage de procéder à des opérations de collecte et de traitement, à savoir : une obligation de déclaration des fichiers d'adresses électroniques (a.), une obligation de sécurité et de confidentialité des données (b.) ainsi qu'une obligation d'informer les personnes concernées des traitements opérés sur leurs données (c.), obligations auxquelles le « spammeur » se soustraira de façon flagrante.

a. L'obligation de déclaration des fichiers d'adresses électroniques

211. Définition. En application de l'article 22 de la loi du 6 août 2004, la mise en œuvre d'un traitement automatisé de données est soumise à une obligation préalable de déclaration auprès de la CNIL [532]. Cette déclaration doit comporter une série d'éléments, notamment l'identité et l'adresse du responsable du traitement, la ou les finalités du traitement, les données à caractère personnel traitées, leur origine et les catégories de personnes concernées par le traitement, la durée de conservation des informations traitées, le service chargé de la mise en œuvre du traitement, les destinataires des données, la fonction de la personne auprès de laquelle s'exerce le droit d'accès et les mesures relatives à l'exercice de ce droit ainsi que les dispositions prises pour assurer la sécurité des traitements et des données, les transferts de données à caractère personnel envisagés à destination d'un État non membre de la Communauté européenne [533]. Cette obligation de déclaration concerne donc toutes les hypothèses de traitement, qu'il y ait ou non sous-traitance, et pèse sur la personne qui a décidé de mettre en œuvre un tel traitement de données, cette dernière étant considérée

[530] Martine BEHAR-TOUCHAIS, « Rapport introductif », *in* « Existe-t-il un principe de proportionnalité en droit privé ? – Colloque Paris V, 20 mars 1998 », *LPA* 30 sept. 1998, n° 117, p. 3 et s., spéc. n° 6 et s.
[531] *Id.*, spéc. n° 12.
[532] Cette obligation de déclaration existait déjà dans la loi de 1978 (art.16) et dans la directive de 1995 (art. 18).
[533] Article 30-I. loi n° 2004-801.

comme juridiquement responsable du contenu de la déclaration [534]. Toutefois, pour les catégories les plus courantes de traitements automatisés, publics ou privés, et dont la mise en œuvre n'est pas susceptible de porter atteinte à la vie privée ou aux libertés, l'article 24 de la loi de 2004 prévoit de simplifier la procédure de déclaration ordinaire. À ce titre, la CNIL est chargée d'établir et de publier des normes destinées à cet effet [535]. La Commission a notamment publié la norme simplifiée n° 48 relative aux traitements automatisés de données à caractère personnel qui ont pour objet la gestion, au sein d'un organisme privé ou public, des fichiers de clients et/ou de prospects [536]. Cette norme s'applique aux traitements permettant les opérations relatives à la gestion des clients (contrats, commandes, livraisons, factures, comptes clients et comptes fidélité), à la prospection (constitution et gestion d'un fichier de prospects), à la cession, la location ou l'échange du fichier clients et de prospects, à l'élaboration de statistiques commerciales et à l'envoi de sollicitations. Les données enregistrées sont celles relatives à l'identité du client (nom, prénoms, date de naissance, adresse, numéros de téléphone, de télécopie, adresse électronique, code interne de traitement permettant l'identification du client), aux moyens de paiement utilisés (RIP ou RIB, numéro de la transaction, numéro de chèque, numéro de carte bancaire), à sa situation familiale (nombre et âge du ou des enfant(s) au foyer, profession, domaine d'activité, catégorie socioprofessionnelle), à sa situation économique et financière, à la relation commerciale (abonnement souscrit, quantité, montant, périodicité, adresse de livraison, historique des achats …) ainsi qu'aux règlements des factures (modalités de règlements, remises consenties, informations relatives aux crédits souscrits …) [537].

212. Qu'en est-il du « spammeur » ? Malgré l'existence de cette obligation et de sa version simplifiée, il semble peu probable que le « spammeur » prenne le soin de l'observer avant la mise en œuvre de tout traitement dans la mesure où ce dernier, dans sa logique de prospection effrénée, ne saurait s'embarrasser de formalités administratives. Or, cet argument commercial ne saurait prospérer en sa faveur et notamment lorsque ce dernier

[534] Celui qui loue un fichier auprès de la personne qui l'a créé en devient responsable et à ce titre, est astreint à cette déclaration et ce, même si le créateur du fichier y avait précédemment procédé.
[535] Il existe également des cas de dispense de déclaration mais que nous n'évoquerons pas ici, leur analyse dépassant le cadre de notre étude. – Pour des précisions sur les normes simplifiées, v. le site de la CNIL accessible à l'adresse suivante : http://www.cnil.fr/en-savoir-plus/deliberations/normes-simplifiees/ et sur l'ensemble des cas de dispense, consulter l'adresse suivante : http://www.cnil.fr/en-savoir-plus/deliberations/dispenses-de-declaration/ ; v. ég. « Tableau récapitulatif, Quelle déclaration pour quel fichier », disponible sur : http://www.cnil.fr/fileadmin/documents/approfondir/dossier/collec/TB-formalites-CL-VD.pdf . – Pour une étude très détaillée de l'ensemble de cette question, v. not. Jean FRAYSSINET, *Atteintes aux droits de la personne résultant des fichiers ou des traitements informatiques*, fasc. préc., spéc. n^{os} 99-151.
[536] CNIL, Délibération n° 2005-112 du 07 juin 2005 portant création d'une norme simplifiée concernant les traitements automatisés de données à caractère personnel relatifs à la gestion des fichiers de clients et de prospects et portant abrogation des normes simplifiées 11, 17 et 25, disponible sur : http://www.cnil.fr/en-savoir-plus/deliberations/deliberation/delib/184/.
[537] *Id.*

bénéficie d'un allègement des formalités de déclaration. En effet, lorsque les traitements envisagés entrent dans le champ de la norme simplifiée n° 48, ce dernier a non seulement moins d'informations à fournir mais la plupart du temps, une seule déclaration sera nécessaire pour tous les traitements du même type. Il en résulte que l'absence de déclaration des traitements envisagés par le « spammeur » est manifestement un signe de mauvaise volonté de sa part d'autant plus incontestable lorsqu'il est seulement soumis à l'accomplissement d'une déclaration simplifiée.

b. Les obligations de sécurité et de confidentialité des données

213. Définition. Rejoignant la lettre de la loi de 1978 [538] et celle de la directive de 1995 [539], l'alinéa 1er de l'article 34 de la loi de 2004 impose au responsable du traitement de prendre « *toutes les précautions utiles* » afin de préserver la sécurité des données nominatives pour « *notamment, empêcher qu'elles soient déformées, endommagées* » ainsi que leur confidentialité. Cette obligation de confidentialité impose que les données soient divulguées aux seules personnes désignées dans la déclaration de traitement adressée à la CNIL et donc autorisées à y avoir accès. Enfin, cette obligation consiste également à maintenir secrètes les données collectées en les codant grâce au recours à un procédé de cryptographie, encore appelé chiffrement [540].

214. Vers une obligation renforcée. La proposition de loi, dite « Détraigne-Escoffier » du nom de leurs auteurs, déposée le 6 novembre 2009 et visant à modifier la loi IFL [541], encourage un renforcement de l'obligation de sécurité et de confidentialité des données en substituant à l'expression « *mesures adéquates* » celle de « *précautions utiles* » qui est plus précise. Cette modification emporterait l'obligation pour le responsable du traitement d'adapter les mesures de sécurité en fonction du type de données et des risques présentés par le traitement considéré. Par ailleurs, le paysage législatif européen a connu des évolutions récentes qui auront un impact sur notre droit national et plus particulièrement sur notre législation en matière de protection des données. En effet, l'adoption de la directive 2009/136/CE [542], modifiant la directive « vie privée et communications électroniques » de

[538] Art. 29 loi n° 78-17 : « *Toute personne ordonnant ou effectuant un traitement d'informations nominatives s'engage de ce fait, vis-à-vis des personnes concernées, à prendre toutes précautions utiles afin de préserver la sécurité des informations et notamment d'empêcher qu'elles ne soient déformées, endommagées ou communiquées à des tiers non autorisés* ».

[539] Art. 17.1 dir. 95/46/CE : « *Les États membres prévoient que le responsable du traitement doit mettre en œuvre les mesures techniques et d'organisation appropriées pour protéger les données à caractère personnel contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisés, notamment lorsque le traitement comporte des transmissions de données dans un réseau, ainsi que contre toute autre forme de traitement illicite* ».

[540] Sur ce procédé, v. par exemple Isabelle ROUJOU DE BOUBEE, « Cryptographie : ses nécessités et ses dérives », *in* Marie-Christine PIATTI, *Les libertés individuelles à l'épreuve des NTIC*, *op. cit.*, spéc. p. 125 et s.).

[541] Yves DETRAIGNE et Anne-Marie ESCOFFIER (présentée par), Proposition de loi visant à mieux garantir le droit à la vie privée à l'heure du numérique, 6 nov. 2009, proposition préc.

[542] Directive 2009/136/CE du Parlement européen et du Conseil du 25 novembre 2009 modifiant la directive 2002/22/CE concernant le service universel et les droits des utilisateurs au regard des réseaux et des services de communications, la directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques et le règlement (CE) n° 2006/2004 relatif à la coopération entre les autorités nationales chargées de veiller à l'application de la législation en matière de protection des consommateurs, J.O.U.E. n° L. 337 du 18 décembre 2009, p. 11 et s. – Cette directive devra être transposée en droit national le 25 mai 2011 au plus tard (art. 4 dir. 2009/136/CE).

2002 [543], vise à renforcer la protection des données personnelles par la création d'une procédure de notification des violations de ces données [544]. Transposant de façon anticipée cette directive, la proposition de loi de novembre 2009 introduirait dans la loi IFL, à l'article 34 alinéa 1er susvisé, la notion de « *violation de données à caractère personnel* » définie par la directive de 2009 comme « *une violation de la sécurité entraînant accidentellement ou de manière illicite la destruction, la perte, l'altération, la divulgation ou l'accès non autorisés de données à caractère personnel transmises, stockées ou traitées d'une autre manière en relation avec la fourniture de services de communications électroniques accessibles au public dans la Communauté* » [545]. Cette définition large permettrait ainsi d'« *englober la plupart des situations pertinentes dans lesquelles la notification des violations de la sécurité pourrait être garantie* » [546]. Tel est le cas par exemple dans l'hypothèse d'un accès non autorisé à des données à caractère personnel lors du piratage d'un serveur contenant ce type de données ou encore la perte ou la divulgation de données sans que l'accès non autorisé n'ait encore été prouvé [547]. L'obligation de sécurité serait ainsi précisée dans les termes suivants : tout responsable de traitement serait tenu d'« *assurer la sécurité des données et en particulier* [de] *protéger les données à caractère personnel traitées contre toute violation entraînant accidentellement ou de manière illicite la destruction, la perte, l'altération, la divulgation, la diffusion, le stockage, le traitement ou l'accès non autorisés ou illicites, particulièrement lorsque le traitement comporte des transmissions de données dans un réseau, ainsi que contre toute autre forme de traitement illicite* » [548]. De surcroît, la

[543] Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques, dir. préc.

[544] Art. 4 dir. 2009/136/ CE ; v. ég. considérant 59 dir. 2009/136/CE : « *L'intérêt des utilisateurs à être informés ne se limite pas, à l'évidence, au secteur des communications électroniques, et il convient dès lors d'introduire de façon prioritaire, au niveau communautaire, des exigences de notification explicites et obligatoires, applicables à tous les secteurs* »). – Sur la réflexion engagée aux fins d'extension de cette obligation de notification des violations de données à tous les secteurs et non plus seulement à celui des communications électroniques en raison des risques que de telles violations se produisent dans d'autres secteurs, notamment financiers (v. en ce sens, Communication de la Commission au Parlement européen, au Conseil et au Comité économique et social européen et au Comité des régions, « Approche globale de la protection des données à caractère personnel dans l'Union européenne », Bruxelles, 4 nov. 2010, COM(2010) 609 final, spéc. p. 7, disponible sur : http://ec.europa.eu/health/data_collection/docs/com_2010_0609_fr.pdf). – Antérieurement, v. not. G29, Avis n° 2/2008 sur la révision de la directive 2002/58/CE, 00989/08/FR, WP 150, 15 mai 2008, spéc. p. 3, disponible sur : http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp150_fr.pdf. – Avis du contrôleur européen de la protection des données sur la proposition de directive du Parlement européen et du Conseil modifiant, entre autres, la directive 2002/58/CE, J.O.U.E. n° C 181 du 18 juillet 2008, p. 1 et s., spéc. n° 30, p. 6, disponible sur : http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2008:181:0001:0001:FR:PDF.

[545] Art. 2 dir. 2009/136/CE complétant ainsi l'article 2 h) dir. 2002/58/CE.

[546] Deuxième avis du contrôleur européen de la protection des données relatif au réexamen de la directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive « vie privée et communications électroniques ») du 9 janvier 2009, J.O.U.E. n° C. 128 du 6 juin 2009, p. 28 et s., spéc. nos 19, p. 30, disponible sur : http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2009/09-01-09_ePricacy_2_FR.pdf.

[547] *Id.* spéc. nos 20-21, p. 30.

[548] Art. 7, al. 2 proposition de loi, 6 nov. 2009, préc. modifiant l'article 34, al. 1er loi n° 2004-801.

proposition de loi précise qu'en cas d'atteinte à la sécurité des données, le responsable de traitement serait tenu d'en alerter « *sans délai* » la CNIL qui pourrait imposer à ce dernier d'en avertir également les personnes physiques concernées [549]. Cette dernière obligation appelle une série d'observations. Tout d'abord, concernant le critère déclenchant cette obligation de notification, à savoir l'atteinte à la sécurité des données, la proposition de loi consacre une acception large puisqu'aucun seuil de gravité de l'atteinte n'est fixé. Cette solution permettrait ainsi de ne pas limiter de manière excessive le nombre de violations pour lequel une notification serait requise. Cette solution est opportune dans la mesure où retenir une conception restrictive de la notion d'atteinte à la sécurité confèrerait au responsable du traitement un large pouvoir d'appréciation pouvant l'inciter à considérer plus fréquemment l'absence de risque grave d'atteinte à la sécurité des données afin d'échapper à cette obligation [550]. Ensuite, s'il appartient au responsable du traitement de déterminer si l'atteinte à la sécurité des données donne lieu à notification, la proposition de loi lui impose d'en informer immédiatement la CNIL. Cette exigence permettrait ainsi d'éviter les éventuels abus grâce à un pouvoir de contrôle conféré à la CNIL. Cette compétence lui permet en effet d'enquêter sur les circonstances de la violation et d'exiger toute mesure corrective susceptible d'être appropriée pour mette fin à cette violation [551]. Un tel pouvoir de supervision lui permettra, le cas échéant, d'imposer au responsable du traitement une notification auprès des titulaires de données concernés [552]. Par ailleurs, concernant les destinataires de la notification, la proposition de loi vise toutes les personnes dont les données ont été compromises par la violation de la sécurité [553], ce qui permet d'englober non seulement les abonnés à un service de communications électroniques accessibles au public,

[549] Art. 7, al. 3 proposition de loi, 6 nov. 2009, préc., s'inspirant de l'article 2.4 c) dir. 2009/136/CE qui ajoute à l'art. 4 dir. 2002/58/CE une nouvelle disposition rédigée dans les termes suivants : « *En cas de violation de données à caractère personnel, le fournisseur de services de communications électroniques accessibles au public avertit sans retard indu l'autorité nationale compétente de la violation. Lorsque la violation de données à caractère personnel est de nature à affecter négativement les données à caractère personnel ou la vie privée d'un abonné ou d'un particulier, le fournisseur avertit également sans retard indu l'abonné ou le particulier concerné de la violation* ».

[550] V. en ce sens, Deuxième avis du contrôleur européen de la protection des données relatif au réexamen de la directive 2002/58/CE, avis préc., spéc. n° 40, p. 33 (à noter toutefois que dans cet avis, le contrôleur européen recommandait une formule prenant en compte le simple risque : la notification serait exigée « *s'il y a des chances raisonnables pour que la violation ait des effets négatifs pour les personnes* », formule plus protectrice que celle retenue par la directive de 2009 et par la proposition de loi de 2009, mais qui pourrait s'exposer à des critiques eu égard à une certaine appréciation subjective qu'elle induit nécessairement).

[551] Art. 2.10. dir. 2009/136/CE insérant l'article 15 bis §3 qui dispose que : « *Les États membres veillent à ce que l'autorité nationale compétente et, le cas échéant, d'autres organismes nationaux disposent des pouvoirs d'enquête et des ressources nécessaires, et notamment du pouvoir d'obtenir toute information pertinente dont ils pourraient avoir besoin, afin de surveiller et de contrôler le respect des dispositions nationales adoptées en application de la présente directive* ».

[552] V. en ce sens la recommandation du contrôleur européen de la protection des données (Deuxième avis préc., spéc. n° 54, p. 34).

[553] Art. 7, al. 3 proposition de loi préc. s'inspirant de l'article 2.3 c) dir. 2009/136/CE : « *Lorsque la violation de données à caractère personnel est de nature à affecter négativement les données à caractère personnel ou la vie privée d'un abonné ou d'un particulier, le fournisseur avertit également sans retard indu l'abonné ou le particulier concerné de la violation* ».

les personnes qui se sont récemment désabonnées mais dont les données à caractère personnel sont encore conservées par le responsable du traitement mais aussi toute personne dont les données auraient été transmises par un abonné de ce service [554]. Eu égard à cette dernière hypothèse, toute atteinte à la sécurité implique d'en informer également ce tiers [555]. Enfin, dans un souci d'efficacité, il convient de souligner que même si la France a échappé pour le moment aux scandales liés à la perte ou à la divulgation illégale des données comme ceux que les États-Unis ont connus [556] ou plus récemment, l'Allemagne et la Grande-Bretagne [557], l'adoption de ces nouvelles dispositions permettrait sans conteste de renforcer le niveau de protection des données assuré par la loi française qui reste encore insuffisant à ce jour. Cette modification aurait en outre le mérite de se rapprocher du système américain, qui sur ce point est nettement plus en avance puisque la majorité des États a déjà adopté des dispositions contraignantes à cet égard [558].

215. Qu'en est-il du « spammeur » ? Il semble que cette obligation ne puisse pas, par définition, être respectée par le « spammeur » puisque ce dernier profite précisément des failles de sécurité des systèmes informatiques pour récolter les données nominatives non protégées, voire revendre ses bases de données d'adresses électroniques collectées, sans se soucier de la sécurité ou de la confidentialité de ces données.

c. L'obligation d'information

216. Une étendue variable. L'obligation d'informer les titulaires de données des traitements opérés est essentielle puisque son respect conditionne l'effectivité de la mise en œuvre des droits reconnus à ces derniers [559]. En effet, sans connaître l'existence des

[554] Cette obligation permet à toute personne concernée d'être informée des violations de sécurité et de prendre les mesures nécessaires pour résoudre les problèmes qui en découlent (v. Avis du contrôleur européen de la protection des données sur la proposition de directive du Parlement européen et du Conseil modifiant, entre autres, la directive 2002/58/CE, avis préc., spéc. n° 29, p. 6).

[555] Également favorable à ce large champ d'application, v. not. G29, Avis n° 2/2008 sur la révision de la directive 2002/58/CE, avis préc., spéc. p. 3. – Deuxième avis du contrôleur européen de la protection des données relatif au réexamen de la directive 2002/58/CE, avis préc., spéc. n[os] 58-59.

[556] Sur ces affaires, v. *infra* : n° 266.

[557] CNIL, *Rapport d'activité 2009*, n° 30, Doc. fr., 2010, spéc. p. 57.

[558] En effet, quarante cinq États sur cinquante ont prévu des dispositions contraignantes en matière de sécurité des données. De même, la proposition de loi américaine de 2009, le *Privacy Act*, impose des obligations similaires en cas d'atteinte à la sécurité des données (sur la législation applicable aux États-Unis en matière de protection des données, v. *infra* : n° 261 et s).

[559] On retrouve une obligation d'information en droit des contrats, la jurisprudence ayant dégagé son existence à partir de l'exigence d'un consentement sain et éclairé qui conditionne la validité des contrats (art. 1108, 1109 C. civ.), mais aussi à partir d'un devoir de loyauté des contractants qui doit exister au moment de la formation du contrat (absence de dol) et lors de son exécution (art. 1116, 1134, al. 2 C. civ.). – De même, l'obligation d'information soumet le vendeur à faire connaître à l'acheteur la portée de ses engagements (art. 1602 C. civ) (v. par ex. Cass. civ. 1re, 13 avr. 1999, *Juris-Data* n° 1999-001623 ; *Cont. conc. conso.* sept. 1999, comm. 127,

traitements réalisés, l'exercice des autres droits – droit d'accès, droit d'opposition et droit de rectification – semble bel et bien compromis [560]. L'étendue de cette obligation peut toutefois varier selon que la collecte est directe ou indirecte [561]. Afin d'en saisir les contours, prenons le cas où une opération de publipostage est envisagée.

217. L'hypothèse de la collecte directe. Le publipostage peut tout d'abord s'opérer à partir d'adresses électroniques communiquées par des clients, prospects ou visiteurs d'un site *Web*, avec qui le prospecteur a été en contact direct. L'envoi de messages est licite si, lors de la collecte initiale des adresses, le prospecteur, responsable du traitement, a communiqué aux titulaires de ces données[562] : l'identité du responsable du traitement, la finalité du traitement, le caractère obligatoire ou facultatif des réponses, les conséquences éventuelles en cas d'absence de réponse, les destinataires des données et les droits dont le titulaire dispose sur ses propres données en vertu de la présente loi et, le cas échéant, les transferts envisagés à destination d'un État non membre de l'Union européenne [563].

218. L'hypothèse de la collecte indirecte. Deux hypothèses sont à distinguer : le publipostage peut être réalisé à partir d'adresses électroniques fournies par un tiers ou aspirées sur les espaces publics de l'internet (forums de discussion, annuaires, réseaux sociaux…). Le premier cas recouvre celui où les fichiers sont constitués à partir d'adresses que le prospecteur s'est procuré auprès d'un tiers. Il en est ainsi, par exemple, lorsqu'un site *Web* a cédé à ce prospecteur les adresses collectées auprès des internautes. Cette cession est licite, sous réserve que ledit site ait communiqué l'ensemble des informations précitées dès la collecte initiale des données aux personnes concernées, et que ces dernières ont été

p. 1819, obs. L. Leveneur.). – V. ég. en droit de la consommation, l'article L. 111-1 du Code de la consommation et de nombreux textes réglementaires obligent le professionnel à informer le consommateur, avant la conclusion du contrat, des caractéristiques essentielles de la chose vendue ou du service rendu.

[560] Sur le contenu de ces droits, v. *infra :* n° 223 et s.

[561] CNIL, *Le publipostage électronique et la protection des données personnelles*, rapport préc., spéc. p. 19 et s.

[562] Art. 32-I loi n° 2004-801. – Les articles 14 et 17 du décret n° 2007-451 du 25 mars 2007 modifiant l'article 90 du décret n° 2005-1309 du 20 octobre 2005 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2004-801 du 6 août 2004 précisent les modalités de mise en œuvre de cette obligation. En pratique, le responsable du traitement informe les personnes concernées sur le support de la collecte ou à défaut, sur un document clair préalablement remis à ces personnes, « *des coordonnées du service compétent auprès duquel elles peuvent exercer leurs droits d'opposition, d'accès et de rectification. Lorsque la collecte des données est opérée oralement à distance, il est donné lecture de ces informations aux intéressés en leur indiquant qu'ils peuvent, sur simple demande, même exprimée oralement, recevoir postérieurement ces informations par écrit* » (art. 90 modifié, al. 1er). Toutefois, les informations peuvent être communiquées par voie électronique sous réserve de l'accord des intéressés (art. 90 modifié, al. 2). Enfin, dans le cas où « *les informations sont portées à la connaissance de l'intéressé par voie d'affichage, il lui est indiqué qu'il peut, sur simple demande orale ou écrite, recevoir ces informations sur un support écrit* » (art. 90 modifié, dernier alinéa).

[563] Lorsque les données ont été recueillies par voie de questionnaires, le contenu de l'information est allégé et porte uniquement sur l'identité du responsable du fichier, la finalité du traitement, le caractère obligatoire ou facultatif des réponses fournies et les droits reconnus à la personne concernée (art. 32-I, dernier alinéa loi n° 2004-801).

informées que leurs données pouvaient être communiquées à un tiers à des fins de prospection, « *au plus tard lors de la première communication des données* » [564]. En revanche, lorsque les données sont aspirées sur les espaces publics de l'internet à l'insu des personnes concernées, la collecte est considérée comme déloyale, le titulaire ne pouvant, par définition, exercer notamment ses droits d'opposition et de rectification [565].

219. Les informations spécifiques relatives au transfert hors Union européenne. Dans le cas où s'opère un transfert de données vers un autre État non membre de l'Union européenne [566], cette obligation est renforcée puisque le responsable du traitement doit apporter à la personne directement concernée par cette opération, outre les informations d'ordre général précitées et visées à l'article 32-I de la loi de 2004, de plus amples informations quant au transfert de données envisagé [567], à savoir : le(s) pays destinataire(s) des données, la nature des données transférées, la finalité du transfert envisagé, la (ou les) catégorie(s) de destinataires et le niveau de protection offert par le(s) pays tiers. Pour les pays tiers reconnus comme offrant un niveau de protection des données suffisant [568], le responsable doit citer la décision de la Commission européenne approuvant le transfert. À défaut d'atteindre le niveau de protection suffisant [569], ce dernier est tenu de mentionner la

[564] Art. 32 III al. 1er loi n° 2004-801.

[565] Sur le caractère déloyal de ce type de collecte, v. *supra* : n° 200.

[566] Art. 68 et s. loi n° 2004-801. – Pour plus de détails sur ces transferts, v not. CNIL, « Transferts de données à caractère personnel vers des pays non membres de l'Union européenne », juin 2008, disponible sur : http://www.cnil.fr/fileadmin/documents/approfondir/dossier/international/Guide-tranfertdedonnees.pdf. – Gaëtan CORDIER, « Les tranferts de données personnelles vers des pays tiers : suivez l'exemple ! », *Comm. com. électr.* juill. 2008, prat. 7, p. 44 et s. – Jean FRAYSSINET, « Le transfert et la protection des données personnelles en provenance de l'Union europenne vers les États-Unis : l'accord dit « sphère de sécurité » (ou safe harbour) », *Comm. com. électr.* mars 2001, chron. 7, p. 10 et s. – Marc-Antoine LEDIEU, « Les transferts internationaux de données à la française », *Comm. com. électr*. janv. 2006, Étude 2, p. 17 et s. – Pierre LECLERCQ, « Loi du 6 août 2004. Transferts internationaux de données personnelles », *Comm. com. électr*. févr. 2005, Étude 8, p. 29 et s. – Yves POULLET, « Pour une justification des articles 25 et 26 de la directive européenne 95/46/CE en matière de flux transfrontalières et de protection des données », *Comm. com. électr*. déc. 2003, chron. 29, p. 9 ; « Flux transfrontalières de données, vie privée et groupes d'entreprises », *RLDI* sept. 2005, n° 236, p. 47 et s. – Chloé TORRES, « Flux transfrontières de données : convention ou règles internes ? », *Gaz. Pal*. 20 juill. 2006, n° 201, p. 11 et s. – Michel VIVANT, « les transferts internationaux de données dans la loi de 2004 », *RLDI* oct. 2005, n° 270, p. 64.

[567] Cette hypothèse doit être envisagée puisque dans le cas du *spamming*, les données sont susceptibles d'être collectées partout dans le monde.

[568] Art. 68 al. 2 loi n° 2004-801 : « *Le caractère suffisant du niveau de protection assuré par un État s'apprécie en fonction notamment des dispositions en vigueur dans cet État, des mesures de sécurité qui y sont appliquées, des caractéristiques propres du traitement, telles que ses fins et sa durée, ainsi que de la nature, de l'origine et de la destination des données traitées* ».

[569] Si le niveau de protection des données à caractère personnel dans l'Union européenne est relativement homogène grâce à la transposition en droit interne de la directive 95/46/CE, la situation est plus disparate dans les autres pays mêmes occidentaux. La CNIL a dressé en 2008 un « Panorama des législations » dans le monde en fonction du niveau des garanties offertes au regard de la législation européenne. Quatre grands groupes s'en dégagent : les États de l'Union européenne qui assurent tous un niveau de protection équivalent ; ceux de l'Espace Économique Européen qui, à l'exception de la Suisse, ont transposé dans leur droit interne la directive 95/46/CE et sont ainsi considérés comme garantissant un niveau de protection équivalent à celui existant dans les pays membres de l'Union européenne ; les pays non membres de l'Union européenne se divisent quant à eux en deux catégories selon qu'il assurent ou non un niveau de protection adéquat (« Panorama des législations », 2

décision de la CNIL autorisant le transfert en application de l'article 69 de la loi de 1978 modifiée [570].

220. Vers une obligation d'information renforcée. La proposition de loi de 2009 envisage de soumettre le responsable du traitement à une obligation d'information plus précise quand aux traitements envisagés en modifiant de façon substantielle l'article 32 de la loi IFL [571]. Outre l'ensemble des éléments précités [572], le responsable qui dispose d'un site *Web* devra délivrer, avant tout traitement de données, une information « *spécifique, claire et accessible* » relative à la durée de conservation des données et à la possibilité pour la personne concernée d'exercer ses droits de suppression, d'accès et de rectification par voie électronique. Ce dernier devra en outre faire figurer l'ensemble de ces informations – les mentions obligatoires prévues au I de l'article 32 auxquelles s'ajoutent à celles fixées par la proposition de loi de 2009 – dans une rubrique « *spécifique, claire, accessible et permanente* ». Enfin, ce même article prévoit un renforcement de l'obligation d'information en matière de *cookies* ou en cas de collecte indirecte.

221. Quid du *spamming* ? Dans la plupart des cas, le « spammeur » a recours à des logiciels destinés à aspirer à l'insu des internautes les adresses électroniques que ces derniers auront communiquées lors des diverses opérations effectuées en ligne et qui circulent dans les espaces publics de l'internet (forums de discussion, liste de diffusion, annuaires, sites *Web*, réseaux sociaux) [573]. Dans ces circonstances, il apparaît incontestable que l'obligation d'information qui incombe au « spammeur » en tant que responsable de traitement est clairement transgressée. Quant à l'obligation renforcée prévue en cas de transfert de données hors Union européenne, celle-ci ne sera évidemment pas davantage respectée.

222. Bilan. À l'issue de cette étude, il convient de constater que la pratique du *spamming* s'exerce en parfaite infraction à la loi IFL, privant ainsi les titulaires des données des droits que leur confère la loi française. En suivant une démarche similaire à celle qui vient d'être adoptée, nous exposerons brièvement le contenu de ces prérogatives légales pour ensuite évaluer dans quelle mesure les droits reconnus aux titulaires des données traitées sont clairement ignorés par les « spammeurs ».

juin 2008, disponible sur : http://www.cnil.fr/fileadmin/documents/approfondir/dossier/international/panorama-legislation.pdf).

[570] Art. 91-5° b) décret n° 2007-451 préc.

[571] Art. 6 proposition de loi, 6 nov. 2009, préc.

[572] V. *supra* : n^os^ 217 à 219.

[573] Sur ce mode de collecte, v. *supra* : n° 92.

B. DES DROITS IGNORES PAR LES « SPAMMEURS »

223. Au-delà des obligations incombant aux responsables de traitements, le législateur a reconnu corrélativement aux titulaires de données nominatives certains droits qui permettent de neutraliser le rapport de force que ces derniers entretiennent avec les premiers. À cet égard, la CNIL, consciente des dérives que pouvait générer une prospection à moindre coût, a encouragé la mise en place d'un système de protection fort au profit de ces titulaires [574]. Il s'agit ainsi d'apprécier l'intensité des menaces que représente le *spamming* pour l'ensemble de ces droits à travers l'examen successif de chacun d'eux, à savoir : le droit d'opposition (1.), le droit d'accès (2.), les droits de rectification et de suppression (3.) et enfin, le droit à l'oubli (4.). À cette occasion, nous préciserons les évolutions susceptibles de voir le jour si la proposition de loi de 2009 [575] visant à renforcer l'exercice de ces droits [576], venait à être adoptée et évaluerons son impact dans la lutte contre le *spamming*.

1. Le non-respect du droit d'opposition, prolongement du devoir d'information

224. Définition et mise en oeuvre. À l'instar de la loi de 1978 [577], la loi de 2004 accorde à toute personne le droit, « *pour des motifs légitimes* », de manifester auprès du responsable du traitement [578], son opposition à ce que ses données fassent l'objet d'un traitement [579]. Ce droit d'opposition doit s'exercer gratuitement [580]. La CNIL précise qu'il

[574] « *Plus le coût de la prospection est faible, plus les risques d'abus sont réels. C'est pourquoi plus le coût de la prospection est faible, plus les droits garantis aux personnes sont forts. Or, la prospection électronique est la moins coûteuse de toutes les formes de prospection existantes. Cette tendance lourde doit également faire partie de la réflexion* » (CNIL, *Le publipostage électronique et la protection des données personnelles*, rapport préc., spéc. p. 6).

[575] Proposition de loi, 6 nov. 2009, préc.

[576] À l'instar du droit de la consommation, cette proposition de loi permettrait aux personnes lésées par un comportement commis en infraction de la loi IFL de saisir la juridiction la plus proche de leur domicile. Cette solution permettrait ainsi de remédier à une situation de blocage qui peut résulter aujourd'hui de l'application des règles du Code de procédure civile selon lesquelles la juridiction compétente est celle du lieu où se situe le siège du responsable du traitement, lieu qui peut être éloigné du lieu de résidence du demandeur (Art. 13 proposition de loi préc).

[577] Art. 26 loi n° 78-17 : « *Toute personne physique a le droit de s'opposer, pour des raisons légitimes, à ce que des informations nominatives la concernant fassent l'objet d'un traitement* ».

[578] Le responsable du traitement doit indiquer les coordonnées du service compétent auprès duquel la personne peut exercer son droit d'opposition. À défaut d'identification possible par le demandeur du responsable, la demande peut être adressée directement au siège de la société qui sera alors « *transmise immédiatement au responsable de traitement* » (art. 14 D. n° 2007-451 du 25 mars 2007 préc. modifiant l'art. 92 alinéa 2 D. n° 2005-1309 préc.). – Le respect de cette obligation est également indispensable pour la mise en œuvre des droits d'accès et de rectification (sur ces droits, v. *infra* : n^{os} 227 à 232).

[579] Art. 38 al. 1er loi n° 2004-801.

[580] Art. 38 al. 2 loi n° 2004-801. – Le décret de 2007 précise que pour faciliter l'exercice du droit d'opposition prévu à l'alinéa 2 de la loi IFL, l'intéressé est mis en mesure d'exprimer son choix avant la validation définitive de ses réponses. Lorsque la collecte des données intervient par voie orale, l'intéressé est mis en mesure d'exercer

existe différentes formes d'expression de ce droit parmi lesquelles figurent notamment le refus de répondre lors d'une collecte non obligatoire de données, la faculté de demander la radiation des données contenues dans des fichiers commerciaux, la possibilité d'exiger la non-cession ou la non-commercialisation d'informations, notamment par le biais d'une case à cocher dans les formulaires de collecte [581]. En cas de collecte directe des données [582], la personne doit être informée, au moment de la collecte initiale de ses données de son droit de s'opposer à ce que celles-ci soient utilisées à des fins de prospection, notamment commerciale [583], et doit être mise en mesure de l'exercer « *dès la collecte et en ligne* » par le biais d'une case à cocher [584]. À défaut d'exercer ce droit, la personne est présumée avoir consenti à la réception de messages publicitaires de la part du prospecteur ou du site *Web* à qui elle a divulgué ses données et ce, tant qu'elle n'a pas signalé son refus de continuer à en être destinataire [585]. Dès que le responsable envisage de communiquer des données nominatives à des tiers [586], il doit en informer au préalable les personnes concernées [587] afin qu'elles puissent, le cas échéant, s'y opposer. Pour assurer l'exercice de ce droit, le responsable doit les avoir mises en mesure de pouvoir s'opposer à cette cession par le biais d'une case à cocher prévue à cet effet. Le responsable du traitement auprès duquel le droit d'opposition a été exercé doit, sans délai, informer de cette décision tout autre responsable de traitement à qui il aurait transmis les données faisant l'objet de cette opposition [588]. L'absence de case cochée vaut consentement de cette dernière à la cession de son adresse à des fins de prospection.

225. Le projet de clarifier et de faciliter le droit d'opposition. L'article 8 de la proposition de loi de 2009 entend préciser et faciliter l'exercice du droit d'opposition en substituant au terme d'« opposition » celui de « suppression ». Il réécrit l'article 38 de la loi IFL en distinguant d'une part, le droit d'opposition qui s'exerce, sans frais, avant tout traitement ou en cas de collecte indirecte, avant toute communication des données à des tiers et d'autre part, le droit de suppression qui s'exerce, par définition, une fois que les données auront été traitées. La personne pourra ainsi demander, pour des motifs légitimes et sans

son droit d'opposition avant la fin de la collecte des données le concernant (Art. 14 D. n° 2007-451 préc. modifiant l'art. 96 D. n° 2005-1309 préc.).

[581] CNIL, « le droit d'opposition », disponible sur : http://www.cnil.fr/vos-libertes/vos-droits/le-droit-dopposition/.

[582] V. *supra* : n^os^ 59 et 217.

[583] Art. 38 al. 2 loi n° 2004-801.

[584] V. CNIL, *Le publipostage électronique et la protection des données personnelles*, rapport préc., spéc. p. 19. – Art. 14 D. n° 2007-451 préc. modifiant l'art. 96 D. n° 2005-1309 préc.

[585] V. CNIL, *Le publipostage électronique et la protection des données personnelles*, rapport préc., spéc. p. 19.

[586] Il s'agit ici de l'hypothèse de la collecte indirecte, v. *supra* : n° 59.

[587] Sur le devoir d'information, v. *supra* : n° 218.

[588] Art. 14 D. n° 2007-451 préc. modifiant l'art. 97 D. n° 2005-1309 préc. – Étant entendu que la personne concernée aura consenti au préalable au transfert de ses données à un autre responsable de traitement.

frais, leur suppression auprès du responsable du traitement, sauf si le traitement considéré répond à une obligation légale ou lorsque l'application de ces dispositions a été écartée par une disposition expresse autorisant le traitement [589]. Enfin, il convient de préciser que la proposition de loi contribue à faciliter la mise en œuvre de ce droit de suppression en permettant de l'exercer par voie électronique dès lors que le responsable du traitement dispose d'un site *Web* [590].

226. *Quid* du *spamming* ? Lorsqu'une personne reçoit des *spams* dans sa boîte électronique, celle-ci est le plus souvent démunie et ne peut exercer de façon effective son droit d'opposition tel qu'il lui est pourtant reconnu par la loi puisque, dans la grande majorité des cas, la collecte est déloyale [591]. En outre, faute de pouvoir identifier le « spammeur » responsable du traitement, les destinataires ne sont pas en mesure de pouvoir exprimer leur désaccord à la réception de nouvelles sollicitations commerciales ou à la cession de leurs données à des tiers. La seule possibilité serait alors de répondre à l'*e-mail* reçu sans toutefois avoir la certitude que l'adresse d'expédition soit valide. En tout état de cause, lorsque cette possibilité existe par le biais de liens de désinscription, ces derniers sont, le plus souvent, inopérants et destinés seulement à confirmer aux « spammeurs » que l'adresse spammée est bien valide [592]. Il en résulte que malgré le renforcement du droit d'opposition par la proposition de loi de 2009, cette évolution risque d'avoir très peu d'impact face au *spamming*, voire aucun.

2. La reconnaissance d'un droit d'accès

227. Contenu. Après avoir donné son consentement préalable au traitement, le titulaire conserve un certain contrôle sur les traitements ultérieurs opérés sur les données, la loi lui octroyant « *un droit de regard sur l'utilisation qui est faite de ces informations* » [593]. Ce droit d'accès lui permet ainsi de connaître la nature exacte des données enregistrées et

[589] L'article 38 serait ainsi modifié : « *Avant tout traitement de données personnelles ou, en cas de collecte indirecte, avant toute communication de données personnelles, toute personne physique est mise en mesure de s'opposer, sans frais, à ce que les données la concernant soient utilisées à des fins de prospection, notamment commerciale, par le responsable actuel du traitement ou celui d'un traitement ultérieur. Lorsque des données personnelles ont été traitées, toute personne physique identifiée a le droit, pour des motifs légitimes, de demander, sans frais, leur suppression auprès du responsable du traitement. Ce droit ne peut être exercé lorsque le traitement répond à une obligation légale ou lorsque l'application de ces dispositions a été écartée par une disposition expresse de l'acte autorisant le traitement* ».
[590] Art. 6 proposition de loi, 6 nov. 2009, préc.
[591] V. *supra* : n° 200.
[592] Sur ce point, v. *supra* : n° 94 et s.
[593] Pour une approche générale de ce droit, v. CNIL, « Guide droit d'accès », 2010, disponible sur : http://www.cnil.fr/fileadmin/documents/Guides_pratiques/CNIL_Droit_d_acces.pdf.

notamment d'en vérifier l'exactitude. L'article 39-I de la loi de 2004, sur le modèle de la directive de 1995 [594], assure en effet à toute personne le droit de demander au responsable du traitement certaines informations relatives aux traitements déjà effectués et notamment la confirmation de l'existence ou non d'un traitement, les informations relatives aux finalités du traitement, les données à caractère personnel utilisées et les destinataires auxquels les données sont communiquées. La demande d'accès aux données peut être effectuée par écrit et une copie des données à caractère personnel peut être obtenue immédiatement, sauf disposition législative ou réglementaire contraire [595]. L'article 39-I susvisé précise également que tout intéressé est autorisé à prendre connaissance de l'intégralité des données le concernant et à en obtenir une copie dont le coût ne peut dépasser celui de la reproduction [596]. Il convient de souligner le pragmatisme du législateur lors de la rédaction de cette disposition. En effet, souhaitant rendre ce droit effectif, imposer un coût prohibitif serait revenu en pratique à priver la personne de tout droit d'accès. Toutefois, il reste permis de s'interroger sur les raisons qui justifient que l'exercice du droit d'accès ne soit pas totalement gratuit dans la mesure où le titulaire des données n'a pas pris l'initiative des traitements [597]. Par ailleurs, pour que ce droit puisse être exercé, il est impératif que le responsable du traitement s'identifie clairement [598] et qu'il prévienne le titulaire des données en cas de changement de responsables ou d'adresses. Enfin, pour que l'intéressé puisse avoir la possibilité d'en prendre pleinement connaissance, le responsable du traitement doit mettre à sa disposition toutes les données le concernant pendant une durée suffisante [599].

228. Vers l'exercice d'un droit d'accès plus aisé. La proposition de 2009 prévoit la possibilité pour la personne concernée d'exercer son droit d'accès par voie électronique lorsque le responsable du traitement dispose d'un site *Web* [600]. En outre, le responsable du traitement interrogé au titre du droit d'accès sera tenu d'indiquer l'origine des données et non plus les seules « *informations disponibles quant à l'origine* » de ces données telles que requises jusqu'à présent [601]. Or, le plus souvent, le responsable du traitement n'est pas en mesure de communiquer de telles informations, faute d'avoir mis en place les dispositions nécessaires et notamment d'avoir constitué un historique des données en cas de collecte

[594] Art. 12 dir. 95/46/CE.
[595] Art. 14 D. n° 2007-451 préc. modifiant l'article 98 alinéas 1 et 2 D. n° 2005-1309 préc.
[596] Art. 39-I, 5°, al. 2 loi n° 2004-801.
[597] À noter cependant que le droit droit d'accès peut se trouver limité dans certains cas. En particulier, le responsable du traitement peut s'opposer aux demandes d'accès qu'il estime « *manifestement abusives, notamment par leur nombre, leur caractère répétitif ou systématique* ». Il est alors prévu qu'« *en cas de contestation, la charge de la preuve du caractère manifestement abusif des demandes incombe au responsable auprès duquel elles sont adressées* » (art. 39-II loi n° 2004-801).
[598] Sur cette obligation d'identification, v. *supra* : n° 211.
[599] Art. 14 D. n° 2007-451 préc. modifiant l'article 98 alinéa 3 D. n° 2005-1309 préc.
[600] Art. 6 proposition de loi, 6 nov. 2009, préc.
[601] Art. 9 proposition de loi, 6 nov. 2009, préc.

indirecte. Cette modification de la loi permettrait ainsi à la personne concernée par le traitement d'identifier le responsable du traitement, détenteur du fichier d'origine et de faciliter l'exercice, auprès de ce dernier, de son droit d'accès et le cas échéant, ses droits d'opposition et de rectification.

229. *Quid* du *spamming* ? Au regard des techniques de collecte des « spammeurs », il semble difficile que le titulaire des données puisse exercer ce droit d'accès de façon effective, quand bien même son exercice en deviendrait facilité. En effet, ignorant l'ampleur, voire le plus souvent l'existence même des collectes réalisées, les titulaires des données se heurtent à une impossibilité matérielle d'accéder à leurs données et d'effectuer un quelconque contrôle sur ces dernières ainsi que sur leur utilisation ultérieure.

3. Le droit de rectification, corollaire du droit d'accès

230. Le droit de rectification : contenu. « *Complément essentiel du droit d'accès* » [602], le droit de rectification permet à toute personne dont les données ont fait l'objet d'un traitement, de pouvoir obtenir leur mise à jour ou leur correction en cas d'erreur, voire leur suppression. Ce droit constitue ainsi un prolongement naturel du droit d'accès sans lequel ce dernier n'aurait aucune raison d'être. À ce titre, l'article 40 de la loi de 2004 impose à tout responsable de traitement de rectifier, compléter, mettre à jour, verrouiller ou effacer « *les données à caractère personnel la concernant, qui sont inexactes, incomplètes, équivoques, périmées, ou dont la collecte, l'utilisation, la communication ou la conservation est interdite* ». Ce même article ajoute qu'à la demande de l'intéressé, le responsable du traitement doit lui démontrer gratuitement qu'il a accompli les opérations auxquelles il devait procéder. En cas de litige, le responsable du traitement doit apporter la preuve qu'il a respecté la demande de rectification [603]. Après avoir effectué ces modifications, ce dernier est tenu d'en informer sans délai les tiers destinataires de ces données qui devront à leur tour accomplir immédiatement les corrections sollicitées [604]. Il convient également d'indiquer que la proposition de loi de 2009 entend faciliter l'exercice du droit de rectification en permettant

[602] V. CNIL, « Le droit de rectification », disponible sur : http://www.cnil.fr/vos-libertes/vos-droits/le-droit-de-rectification/.
[603] Art. 40 al. 3 loi n° 2004-801.
[604] Art. 14 D. n° 2007-451 préc. modifiant l'article 99 D. n° 2005-1309 préc.

à tout intéressé d'en faire la demande par voie électronique dès lors que le responsable du traitement dispose d'un site *Web* [605].

231. Le droit de contestation, prolongement du droit de rectification. Le droit de rectification est prolongé par un droit de contestation consacré à l'alinéa 3 de l'article 40 précité. Dans le cas où « *une donnée a été transmise à un tiers, le responsable du traitement doit accomplir les diligences utiles afin de lui notifier les opérations qu'il a effectuées* » [606].

232. *Quid* du *spamming* ? En tant que corollaires du droit d'accès, il découle nécessairement de la conclusion précédente que les droits de rectification et de contestation, s'ajoutent à la liste des droits violés par les « spammeurs ».

4. Le droit à l'oubli numérique, une prérogative ignorée par le droit ?

233. L'enjeu de la reconnaissance d'un droit à l'oubli. Comme nous l'avons constaté à plusieurs reprises, les progrès technologiques sont porteurs de risques pour les données nominatives, en particulier pour les adresses électroniques communiquées par les internautes au fil de leurs multiples pérégrinations sur l'internet. La vocation naturelle de ces données à circuler sur le réseau les expose inexorablement à des collectes massives à l'insu de leurs titulaires à des fins de traitements très divers. L'enjeu du droit à l'oubli sur l'internet est donc clair : il s'agit de « *retraduire* [dans le monde numérique] *une fonction naturelle, l'oubli, qui fait que la vie est supportable* » [607]. Au regard des dangers de la mémoire informatique, la consécration légale du droit à l'oubli dans l'environnement numérique, entendu comme une limitation temporelle aux traitements opérés, permettrait ainsi de protéger juridiquement les titulaires de données contre l'immense capacité de stockage de l'informatique. C'est dans ce souci de protection des titulaires des données que la CNIL défend clairement et fermement la promotion de ce droit en considérant qu'il « *touche au plus profond de l'identité humaine* » et a vocation à « *éviter d'attacher aux personnes des étiquettes définitives qui portent atteinte à leur capacité de changement et au sentiment le plus intime de leur liberté* » [608]. À cet égard, la Commission a notamment recommandé que

[605] Art. 6 proposition de loi, 6 nov. 2009, préc.
[606] Art. 40 al. 5 loi n° 2004-801.
[607] Alex TÜRK, président de la CNIL, *in* Jean-Baptiste CHASTANT, « La délicate question du droit à l'oubli sur Internet », 12 nov. 2009, disponible sur : http://www.lemonde.fr/technologies/article/2009/11/12/la-delicate-question-du-droit-a-l-oubli-sur-internet_1266457_651865.html
[608] CNIL, *Dix ans d'informatique et libertés*, Economica, 1988, Paris, spéc. p. 18. – CNIL, « Pas de liberté sans droit à l'oubli dans la société numérique », 27 nov. 2009, disponible sur :

« *les éditeurs de bases de données de décisions de justice accessibles sur les sites Internet s'abstiennent, dans un souci du respect de la vie privée des personnes physiques concernées et de l'indispensable " droit à l'oubli ", d'y faire figurer le nom et l'adresse des parties au procès ou des témoins* » [609]. De même, la Commission avait fixé à un mois la durée de conservation des images et sons enregistrés par un système de vidéosurveillance [610]. Dans le dernier rapport annuel de la CNIL, Alex TÜRK, Président de la Commission, estime que « [i]*l est inacceptable et dangereux que l'information mise en ligne sur une personne ait vocation à demeurer fixe et intangible, alors que la nature humaine implique, précisément, que les individus changent, se contredisent, bref, évoluent tout naturellement* » [611]. La CNIL, soutenue par une partie de la doctrine et des praticiens du droit [612], prend ainsi le contre-pied

---

http://www.cnil.fr/la-cnil/actu-cnil/article/article/pas-de-liberte-sans-droit-a-loubli-dans-la-societe-numerique/. – *Rapport d'activité* 2009, rapport préc., spéc. p. 29 et p. 34. – V. ég. en ce sens Pierre KAYSER qui estime que « [l]*'oubli est une valeur essentielle, il tient à la nature même de l'homme et refuser un droit à l'oubli c'est nourrir l'homme des remords, qui n'a d'autre avenir que son passé, dressé devant lui comme un mur qui bouche l'issue* » (*La protection de la vie privée par le droit : Protection du secret de la vie privée*, (préf. Henri MAZEAUD), 3e éd., Économica- P.U.A.M., 1995).

[609] CNIL, délibération n° 01-057 du 29 novembre 2001 portant recommandation sur la diffusion de données personnelles sur internet par les banques de données de jurisprudence ; délibération n° 88-052 du 10 mai 1988 portant adoption d'une recommandation sur la compatibilité entre les lois n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, et n° 79-18 du 3 janvier 1979 sur les archives ; *Rapport d'activité 2003*, n° 24, Doc. fr., 2004, spéc. p. 186 (à l'occasion d'une réflexion engagée sur les listes noires, la CNIL a expressément visé le droit à l'oubli tout en soulignant l'intérêt de sa protection : « *La fixation de la durée de conservation et l'existence de procédés de mise à jour doivent permettre le respect du principe du " droit à l'oubli "* »).

[610] CNIL, délibération n° 92-126, 10 nov. 1992, Doc. fr. 1993, spéc. p. 46.

[611] CNIL, *Rapport d'activité 2009*, rapport préc., spéc. p. 29.

[612] V. not. Alain BENSOUSSAN, avocat spécialiste du droit des nouvelles technologies, a déclaré que « *cette perte de mémoire a vocation à protéger l'individu par rapport à son passé : " il devient le seul archiviste de son histoire personnelle "* » (« Le " droit à l'oubli " sur Internet », *Gaz. Pal.* 6 févr. 2010, p. 3 et s. ; audition par le Sénat dans le cadre du rapport n° 441, spéc. p. 104, disponible sur : www.alain-bensoussan.com/documents/257542.pdf). – Joël BOYER, magistrat et Secrétaire général de la CNIL, estimait que : « [a]*vec une technologie aussi édifiante que celle à laquelle recourt internet, ce droit à l'oubli est essentiel si l'on souhaite que ce monde virtuel obéisse aux règles qui régissent le monde réel* » (« La révolution d'internet », *LPA* 10 nov. 1999, n° 224, p. 11 et s., spéc. p. 15). – Militant fermement en faveur du droit à l'oubli, v.Catherine COSTAZ, « Le droit à l'oubli », *Gaz. Pal.* 27 juill. 1995, doctr., p. 961 et s., spéc. p. 963 (qui estime que l'individu ne saurait pouvoir être enfermé dans une image immuable : « *le passé n'emprisonne pas la personnalité dans un moule façonné de manière définitive* ». Ainsi, « *l'affirmation d'un droit à l'oubli exprime la reconnaissance des mutations de l'être, parce que le présent et l'avenir ne se reflètent pas dans le miroir du passé* »). – Marie-Pierre FENOLL-TROUSSEAU, « Les moteurs de recherche : un piège pour les données à caractère personnel », *Comm. com. élect.* janv. 2006, Étude 3, p. 22 et s., spéc. n° 13. – Daniel GUTMANN, *Le sentiment d'identité, op. cit.*, spéc. n° 283, pp. 245-246. – Gérard HASS et Olivier DE TISSOT, « Le paradoxe du "droit à l'oubli" », *Expertises* mars 2005, p. 104. – De même, selon le professeur Agathe LEPAGE, « [i]*l y a des raisons profondes de se montrer favorable à ce droit* » et elle ajoute que « [l]*a réticence à l'égard du droit à l'oubli apparaît particulièrement mal venue quand elle est envisagée au regard de la jurisprudence sur la " redivulgation " : le fait qu'une personne ait spontanément fait des révélations sur sa vie privée ne dispense pas de solliciter son autorisation pour reprendre ces informations* » (note sous CA Paris, 14e ch. A, 13 sept. 2000, *D.* 2001, somm., p. 2079). – V. ég. Roseline LETTERON, « Le droit à l'oubli », *Rev. dr. publ.* 1996, p. 385 et s., spéc. p. 423 (considérant qu'« [u]*ne consécration formelle* [du droit à l'oubli] *aurait* […] *pour effet de clarifier à la fois sa signification et sa fonction propre. Elle permettrait notamment à l'intéressé de s'en prévaloir lors d'un conflit sans qu'il soit obligé de démontrer au préalable l'existence d'un préjudice* »). – Le professeur Jacques RAVANAS considère que : « [r]*efuser le droit à l'oubli, au mépris de toute " prescription du silence ", c'est nourrir l'homme du remord qui n'a d'autre avenir que son passé, dressé devant lui comme un mur qui bouche l'issue* » (note sous Cass. civ. 1re, 20 nov. 1990, *Mme Monanges c/ Kern et a.* (sur cet arrêt, v. *infra* : note 614), *JCP* 1992, éd. G., II. 21908, spéc. n° 10). – V. ég. Louis-Xavier RANO, La force du droit à l'oubli, Mémoire DEA Montpellier, 2004, sous la direction de Jean FRAYSSINET.

d'un droit positif frileux à sa reconnaissance officielle et d'une jurisprudence qui reste, pour le moment, divisée sur cette question [613]. Afin d'appuyer ce mouvement, il serait dès lors fortement souhaitable que le droit à l'oubli soit « *considéré avec sérieux* » dans le cadre de la réforme de la directive 95/46/CE prévue pour le second semestre de 2011, comme le préconise le professeur Jean FRAYSSINET [614].

234. Un droit sous-jacent dans diverses dispositions légales. Si le droit à l'oubli n'est pas expressément consacré par la loi, diverses expressions de ce « *pseudo-droit à l'oubli* » [615] se manifestent à travers plusieurs dispositions législatives [616], « [c]*e droit à*

[613] Certains juges ont été réfractaires à la reconnaissance d'un droit à l'oubli, v. not. CA Paris, 15 déc. 1967, *JCP* 1967, éd. G., II. 15107, note H.B. ; *RTD civ.* 1971, p. 114, obs. R. Nerson. –TGI Paris, 27 févr. 1970, *JCP* 1970, éd. G., II. 16293, note R. Lindon. – TGI Paris, réf., 6 déc. 1979, *D.* 1980, jurispr., p. 150, note R. Lindon (« *le désir de la demanderesse, légitime en soi, ne saurait s'analyser en un " droit à l'oubli ", qui ne serait réalisé, par la voie judiciaire, qu'au prix d'une atteinte majeure et définitive au principe de la liberté de la presse et à la nécessaire protection d'une œuvre de l'esprit, l'auteur de l'ouvrage ayant voulu " dire la vérité ", ce qui impliquait nécessairement la mise en cause de sa compagne* »). – Cass. civ. 1re, 3 déc. 1980, *aff. Le pull-over rouge*, *D.* 1981, jurispr., p. 221, note B. Edelman. – Cass. civ. 1re, 16 oct. 1984, *JCP* 1984, éd. G., IV. 357. – V. Cass. civ. 1re, 20 nov. 1990, *Mme Monanges c/ Kern et a.*, arrêt préc. (se prononçant également clairement contre la reconnaissance d'un droit à l'oubli : « *les faits touchant à la vie privée de Mme Monanges avaient été livrés, en leur temps, à la connaissance du public par des comptes rendus de débats judiciaires parus dans la presse locale ; qu'ainsi ils avaient été licitement révélés et, partant, échappaient à sa vie privée, Mme Monanges ne pouvant se prévaloir d'un droit à l'oubli pour empêcher qu'il en soit, à nouveau, fait état* »). – V. cependant, l'analyse nuancée du professeur Roseline LETTERON qui estime que la rigueur de la Cour de cassation dans l'affaire *Monanges* ne doit pas s'analyser comme une renonciation définitive à la notion même de droit à l'oubli. Pour appuyer son raisonnement, elle fait remarquer que « *la Cour prend le soin de mentionner qu'en l'espèce les faits étaient " relatés avec objectivité et sans intention de nuire, et qu'ils avaient été livrés à la connaissance du public par des comptes rendus de débats judiciaires contenus dans la presse locale* " ». Elle en déduit ainsi qu'« [a] *contrario, rien n'interdit de penser que le droit à l'oubli aurait pu être admis si les faits avaient été divulgués dans l'intention de nuire ou s'ils n'avaient pas fait l'objet d'une première divulgation licite. Constater qu'un requérant ne peut se prévaloir d'un droit ne signifie pas que ce droit n'existe pas* » (« Le droit à l'oubli », chron. préc., spéc. pp. 412-413. – *Contra* certaines juridictions du fond qui se sont prononcées en faveur la reconnaissance d'un droit à l'oubli, en s'opposant à la redivulgation de faits anciens et ce, même dans le cas où ces derniers auraient été révélés en audience publique ou à l'occasion d'un compte rendu judiciaire, v. not. TGI Paris, 20 avr. 1983, *JCP* 1985, éd. G., II. 20434, obs. R. Lindon (selon le tribunal, « [c]*e droit à l'oubli, qui s'impose à tous, y compris aux journalistes, doit également profiter à tous, y compris aux condamnés qui " ont payé leur dette à la société " et tentent de s'y réinsérer* »). – TGI Paris, 25 mars 1987, *D.* 1988, somm., p. 198, obs. D. Amson (« *Toute personne qui s'est trouvée associée à un événement public, même si elle en a été le protagoniste, est fondée à revendiquer un droit à l'oubli et à s'opposer au rappel d'un épisode de son existence* »). – CA Versailles, 14 sept. 1989, *Jamet, Tesson et a. c/ consorts Girard*, arrêt préc. (« *par l'écoulement d'un temps suffisamment long,* [un procès criminel, évènement public] *peut redevenir, pour la personne qui en a été le protagoniste, un fait de vie privée, rendu au secret et à l'oubli* »). – CA Paris, 1re ch. B, 15 sept. 2000, *SNC Hachette Filipacchi c/ Larissa Vadko-Zschech*, *Gaz. Pal.* 26-27 sept. 2001, 2, somm., p. 1527, note D. Amson (« *l'atteinte* [au droit à l'oubli] *n'est pas minimisée du fait de la publication, à l'époque, par les médias, de photographies et d'articles relatant cette affaire ; qu'elle ne l'est pas non plus en raison de la publication par l'intimée d'un ouvrage relatif aux faits* »).

[614] Jean FRAYSSINET, « Le pseudo droit à l'oubli appliqué à la presse », *Légipresse* oct. 2010, p. 273 et s., spéc. p. 275. – Pour sa part, la Commission européenne, afin de renforcer la protection des droits des personnes et permettre aux intéressés d'exercer un meilleur contrôle sur les données les concernant, étudiera les moyens permettant de « *clarifier le " droit à l'oubli ", c'est-à-dire le droit en vertu duquel les personnes peuvent obtenir l'arrêt du traitement des données les concernant et l'effacement de celles-ci lorsqu'elles ne sont plus nécessaires à des fins légitimes* » (« Une approche globale de la protection des données à caractère personnel », COM (2010) 609 final, 4 novembre 2010, spéc. pp. 8-9, disponible sur : http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_fr.pdf).

[615] Jean FRAYSSINET, « Le pseudo droit à l'oubli appliqué à la presse », *ibid.*

[616] En 2009, le tribunal de grande instance de Paris a clairement énoncé que « *si aucune norme n'édicte au profit des personnes concernées un droit à l'oubli, de nombreuses dispositions légales consacrent un tel principe,*

l'oubli , n'[étant] *pas nouveau* » [617]. À ce titre, on peut citer les dispositions intéressant la prescription, notion fortement imprégnée d'une référence temporelle [618] mais également les effets de l'amnistie [619], de la révision [620], du relèvement [621] ou de la réhabilitation [622] ou encore l'exception de vérité [623]. La prescription permet « *notamment d'empêcher que l'individu soit gêné toute sa vie durant par des informations fichées et utilisées à son insu* » [624] et poursuit en précisant qu'il s'agit d'un droit « *à l'habeas corpus ou d'un droit à l'oubli* » [625].

235. Droit à l'oubli et loi IFL. Si ce droit est apparu avant la loi de 1978, cette dernière a fortement contribué à sa mise en œuvre. Historiquement, l'exercice de cette prérogative est principalement réalisée à travers la limitation de la durée de conservation des données initialement fixée par l'article 28 de la loi de 1978 qui disposait que « *les informations ne doivent pas être conservées sous une forme nominative au-delà de la durée prévue à la demande d'avis ou à la déclaration, à moins que leur conservation ne soit*

telles les règles générales qui régissent les traitements de données à caractère personnel, l'effacement de certaines condamnations du casier judiciaire, la réhabilitation, l'impossibilité de rapporter la preuve d'un fait diffamatoire vieux de plus de dix ans quand l'imputation ne relève d'un débat d'intérêt public, la prohibition de principe du rappel de condamnations amnistiées quand ces dernières ne touchent pas un homme public, la prescription de l'action publique ou des actions civiles en toute matière sauf les crimes contre l'humanité, etc. » (TGI Paris, ord. réf. 25 juin 2009, *Vernes c/* SAS *Les Échos*, *Légipresse* nov. 2009, n° 266, p. 215 et s., note N. Mallet-Poujol). – V. ég. Joël BOYER observe à ce titre que « *l'amnistie efface l'infraction*, […] *la réhabilitation est une manière d'oubli collectif lorsque le condamné n'a pas récidivé, certaines condamnations peuvent être effacées après un temps d'épreuve, l'action publique contre les crimes et délits se prescrit, la condamnation elle-même se prescrit et ne peut plus être exécutée lorsque trop de temps s'est écoulé depuis son prononcé* » (« La révolution d'internet », art. préc., *loc. cit.*). – François PETIT, « La mémoire en droit privé », *RRJ* 1997-1, p. 17 et s., spéc. pp. 32-34 – Roseline LETTERON, « Le droit à l'oubli », préc., spéc. pp. 409-412. – Haritini MATSOPULOU, « L'oubli en droit pénal » *in Les Droits et le Droit, Mélanges dédiés à Bernard BOULOC*, Dalloz, 2007, p. 771 et s.

[617] Joël BOYER, « La révolution d'internet », art. préc., spéc. p. 15.

[618] En droit pénal, le délai de prescription est de vingt ans pour un crime (art. 133-2 C. pén.), cinq ans pour un délit (art. 133-3 C. pén.) et trois ans pour une contravention (art. 133-4 C. pén.) (v. Jean PRADEL, *Droit pénal général*, 17e éd., Cujas, coll. *Manuels*, 2008, spéc. n° 824 et s., pp. 736-739). – En droit civil, la prescription extinctive est de cinq ans pour les actions personnelles ou mobilières (art. 2224 C. civ.). L'action en responsabilité dirigée contre les personnes ayant représenté ou assisté les parties en justice se prescrit par cinq ans (art. 2225 C. civ.), celle née à raison d'un événement ayant entraîné un dommage corporel se prescrit par dix ans (art. 2226, al. 1er C. civ.). En revanche, en cas de préjudice causé par des tortures ou des actes de barbarie, ou par des violences ou des agressions sexuelles commises contre un mineur, l'action en responsabilité civile est prescrite par vingt ans. Quant au droit de propriété, celui-ci est imprescriptible sous réserve que les actions réelles immobilières se prescrivent par trente ans à compter du jour où le titulaire d'un droit a connu ou aurait dû connaître les faits lui permettant de les exercer (art. 2227 C. civ.). – En matière commerciale, la prescription est de cinq ans pour les obligations nées à l'occasion de leur commerce entre commerçants ou entre commerçants et non commerçants (art. L. 110-4, al. 1er C. comm.).

[619] Art. 769, al. 3 C. proc. pén. (v. Jean PRADEL, *Droit pénal général, op. cit.*, spéc. n° 846 et s., pp. 752-755).

[620] Art. 622 et s. C. proc. pén.

[621] Art. 132-21, al. 2 C. pén. et 702-1 C. proc. pén. (v. Jean PRADEL, *Droit pénal général, ibid.*, spéc. n° 859 et s., pp. 762-767.

[622] Art. 133-12 et s. C. pén. – Art. 782 et 783 C. proc. pén. (v. Jean PRADEL, *Droit pénal général, ibid.*, spéc. n° 849 et s., pp. 755-762).

[623] En matière de presse, l'article 35 de la loi du 29 juillet 1881 interdit l'*exceptio veritatis* pour les faits de plus de dix ans.

[624] Jean FRAYSSINET, *Informatique, fichiers et libertés, op. cit.*, spéc. n° 175, p. 74.

[625] *Ibid., loc. cit.*

autorisée par la commission »[626]. Conformément à cette disposition, il est impératif que l'informatique ne donne pas l'opportunité de conserver en mémoire les données nominatives de façon indéfinie. Dans la même veine, la loi de 2004 a repris à son compte cette notion dans un chapitre intitulé « Conditions de licéité des traitements de données à caractère personnel »[627] mais toujours de façon incidente, en disposant que ces données « *sont conservées sous une forme permettant l'identification des personnes concernées pendant une durée qui n'excède pas la durée nécessaire aux finalités pour lesquelles elles sont collectées et traitées* »[628]. Ce droit se trouve ainsi circonscrit en considération du principe de finalité, les données ne pouvant être conservées que pour la durée nécessaire à la réalisation de la finalité expressément visée : au-delà de cette durée, la donnée doit être effacée ou rendue anonyme. Toutefois, malgré ce principe de conservation des données limitée dans le temps, force est de constater que la loi française ne permet pas d'établir un véritable droit à l'oubli numérique puisqu'aucun réel délai de prescription ni aucun droit à la destruction des données ne sont consacrés. Par ailleurs, d'autres dispositions de la loi IFL concourent à l'institution d'un droit à l'oubli. Aux termes de son article 40, toute personne peut exiger du responsable du traitement que ses données soient, selon les cas, rectifiées, complétées, mises à jour, verrouillées, ou effacées si ces dernières sont incomplètes, inexactes, équivoques, périmées ou si leur collecte, leur communication, leur utilisation ou encore leur conservation est interdite. On le constate ainsi, la mise en œuvre de ce droit d'accès ou de rectification se

---

[626] Jean FRAYSSINET, « La loi du 6 janvier 1978, Informatique, fichiers et libertés : Présentation pédagogique et synthétique », chron. préc., spéc. p. 218. – Participant également à l'existence d'un droit à l'oubli, la Convention 108 du Conseil de l'Europe du 28 janvier 1981, suivant la même ligne directrice que la loi de 1978, énonce que « [l]*es informations sont conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire aux finalités pour lesquelles elles sont enregistrées* » (Art. 5 e. Convention 108). Plus loin, faisant écho à l'article 34 de la loi de 1978, cette Convention prévoit que toute personne peut « *obtenir, le cas échéant, la rectification de ces données ou leur effacement lorsqu'elles ont été traitées* ». – Cette limitation de la durée de conservation des données se retrouve dans d'autres domaines. On peut songer par exemple au fichier national automatisé des empreintes génétiques et du service central de préservation des prélèvements biologiques dont la durée de conservation est limitée à quatre ans (art. R. 53-14 C. procédure pénale) ou aux données des dossiers passagers (données PNR (*Passenger Name Record*)). Concernant cette dernière hypothèse, par un accord conclu le 26 juillet 2007, l'Union européenne s'engage à ce que les transporteurs aériens assurant un service de transport international de passagers à destination ou au départ des États-Unis rendent disponibles les données PNR stockées dans leurs systèmes de réservation : « *VI. Le DHS conserve les données PNR de l'UE dans une base de données analytique active pendant sept ans, après quoi les données acquerront un statut inactif, non opérationnel.* […] *Les données PNR de l'UE devraient être détruites à la fin de cette période* […]. *Les données qui sont liées à un cas ou une enquête spécifiques peuvent être conservées dans une base de données active jusqu'à ce que le cas ou l'enquête soient archivés* » (Décision 2007/551/PESC/JAI du Conseil du 23 juillet 2007 relative à la signature, au nom de l'Union européenne, d'un accord entre l'Union européenne et les États-Unis d'Amérique sur le traitement et le transfert de données des dossiers passagers (données PNR) par les transporteurs aériens au ministère américain de la sécurité intérieure (DHS) (accord PNR 2007) - Accord entre l'Union européenne et les États-Unis d'Amérique sur le traitement et le transfert de données des dossiers passagers (données PNR) par les transporteurs aériens au ministère américain de la sécurité intérieure (DHS) (accord PNR 2007), J.O.U.E. n° L 204 du 4 août 2007, p. 16 et s.).

[627] Chapitre 2 loi n° 2004-801.

[628] Art. 6-5° loi n° 2004-801. – Marie-Pierre FENOLL-TROUSSEAU et Gérard HAAS, *Protection des données à caractère personnel – Vie privée et communication électronique*, *J.-Cl. Communication*, Fasc. 4735, 2005, spéc. n° 70 (consiste en « *une limitation dans le temps de la conservation des données à caractère personnel stockées dans la mémoire des ordinateurs* »).

« *rapproche fortement d'un vrai droit à l'oubli* » [629]. Enfin, l'existence du droit à l'oubli peut également procéder, de façon plus radicale, d'autres droits reconnus par la loi IFL qui « *articulés les uns aux autres* […] *permettraient comme le fait effectivement la CNIL, de donner de la substance juridique et opérationnelle à un vrai droit à l'oubli* » [630]. Tel est le cas par exemple du droit d'opposition qui autorise toute personne à interdire la collecte, la mémorisation ou l'utilisation des informations [631]. De même, l'article 8, alinéa 1er de la loi IFL modifiée interdit, sauf consentement exprès de l'intéressé, de collecter ou de traiter des données à caractère personnel qui font apparaître, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou qui sont relatives à la santé ou à la vie sexuelle de celles-ci. Pour sa part, l'article 9 prévoit que les traitements de données à caractère personnel relatifs aux infractions, condamnations et mesures de sûreté ne peuvent être que limitativement mis en œuvre notamment par les juridictions, les autorités publiques ou les auxiliaires de justice, sociétés de perception et de répartition des droits d'auteur et des droits des artistes-interprètes et des producteurs de phonogrammes et de vidéogramme. Enfin, l'article 7 alinéa 5 soumet le traitement de données à caractère personnel au respect d'un équilibre entre la « *réalisation de l'intérêt légitime poursuivi par le responsable du traitement* » et « *l'intérêt ou les droits et libertés fondamentaux de la personne concernée* ».

236. Des initiatives techniques et autorégulatrices soutenant la reconnaissance d'un droit à l'oubli. Certains sites de réseaux sociaux ou des moteurs de recherche œuvrent à améliorer la transparence dans l'utilisation des données à caractère personnel en permettant notamment aux internautes de supprimer les données les concernant. On peut à cet égard citer *Skyrock*, un site de réseau social dédié aux adolescents qui leur propose un service leur permettant de construire un *blog* destiné à créer des profils et à communiquer avec leurs amis [632] et leur offre la possibilité de supprimer gratuitement les comptes qu'ils ont créés [633]. De même, le moteur de recherche *Google* a lancé, en novembre 2009, le service *Google Dashboard*, tableau de bord qui rassemble en un même endroit toutes les données nominatives collectées et stockées par GOOGLE lors de l'utilisation par l'internaute de ces différentes applications proposées par GOOGLE (historique des conversations sur *GTalk*, album photos sur *Picasa Album Web*, vidéos sur *Youtube*, historique de recherches, *e-mails*

[629] Jean FRAYSSINET, « Le pseudo droit à l'oubli appliqué à la presse », chron. préc., spéc. p. 178.
[630] Sur l'incursion de « *manière plus radicale* » du droit à l'oubli dans divers droits octroyés au titulaire des données à caractère personnel par la loi IFL, v. Jean FRAYSSINET, « Le pseudo droit à l'oubli appliqué à la presse », chron. préc., spéc. p. 179.
[631] Art. 38 loi n° 2004-801.
[632] Disponible sur : http://www.skyrock.com/.
[633] V. la page disponible à l'adresse suivante : http://www.skyrock.com/safety/.

sur *Gmail*, recherches d'itinéraires sur *Google Maps*¸…). Grâce à ce service, l'utilisateur peut ainsi accéder à toutes ses informations personnelles qui ont été collectées afin, le cas échéant, de les corriger, d'en restreindre l'accès ou encore de les supprimer [634]. Autre exemple, le célébrissime réseau social *Facebook* qui, initialement, ne permettait à ses utilisateurs que la désactivation de leur compte, leur propose désormais de supprimer définitivement leur profil [635]. Enfin, la mise en œuvre d'un droit à l'oubli numérique s'est également manifestée lors de l'adhésion d'une dizaine de représentants de sites collaboratifs (forums de discussion, *blog* et réseaux sociaux) et de moteurs de recherche à une charte de bonnes pratiques, proposée par Madame Nathalie KOSCIUSKO-MORIZET, secrétaire d'État chargée de la Prospective et du Développement de l'Économie numérique, le 13 octobre 2009 et qui a fait du droit à l'oubli une priorité [636] et à laquelle a adhéré une douzaine de signataires. Cette adhésion emporte pour les réseaux sociaux l'engagement de leur part de créer une sorte de « bureau de réclamations » virtuel permettant de centraliser les demandes de modification ou de suppression d'un compte. Quant aux moteurs de recherche, en se ralliant à cette charte, ces derniers acceptent de supprimer plus rapidement le cache des pages indexées, en particulier lorsque les contenus figurent sur des sites de réseaux sociaux. Parmi les signataires, on peut mentionner les réseaux sociaux *Skyrock* ou Copains d'avant, le moteur de recherche *Bing* de MICROSOFT ou encore le service des pages jaunes ; les grands absents étant pour le moment *Facebook* et *Google* [637].

237. Vers une consécration officielle ? La nécessité de reconnaître officiellement un droit à l'oubli rejoint les évolutions qui se dessinent actuellement tant en jurisprudence qu'au sein de débats parlementaires salués par la CNIL. En effet, en 2009, le tribunal de grande instance de Paris a rompu avec la jurisprudence dominante qui refusait de consacrer

[634] Pour une démonstration très claire du fonctionnement de *Google Dashboard*, consulter la page disponible sur : http://www.google.com/support/accounts/bin/answer.py?hl=fr&answer=162744. – Pour connaître la démarche à suivre pour supprimer le compte ou d'autres données, consulter les pages disponibles sur : http://www.google.com/support/accounts/bin/answer.py?answer=32046&cbid=-1gjmaaepujmzr&src=cb&lev=%20answer; http://www.google.com/support/accounts/bin/answer.py?answer=81987&cbid=-1kectpt9emsiz&src=cb&lev=%20answer.

[635] En se rendant sur la page permettant de se connectant à son compte (disponible sur : http://www.facebook.com/login.php) et après avoir renseigné ses identifiants, apparaît alors la rubrique intitulée « Supprimer mon compte » où il est indiqué : « *Si vous pensez ne plus jamais utiliser Facebook et souhaitez supprimer votre compte, nous pouvons le retirer de nos systèmes. Vous ne pourrez cependant pas réactiver votre compte ni en récupérer le contenu. Si vous souhaitez supprimer votre compte, cliquer sur Envoyer* ».

[636] À noter que Nathalie KOSCIUSKO-MORIZET a également organisé un atelier de réflexion intitulé « Droit à l'oubli numérique » le 12 novembre 2009 (programme disponible sur : http://www.strategie.gouv.fr/article.php3?id_article=1072) ainsi qu'une consultation publique destinée à l'échange d'idées afin d'enrichir la charte sur le droit à l'oubli numérique. – V. ég. Maryse GROS, « Nathalie KOSCIUSKO-MORIZET veut concrétiser le droit à l'oubli », 12 nov. 2009, disponible sur : http://www.lemondeinformatique.fr/actualites/lire-nathalie-kosciusko-morizet-veut-concretiser-le-droit-a-l-oubli-numerique-29416-page-2.html.

[637] Disponible sur : http://www.gouvernement.fr/gouvernement/charte-du-droit-a-l-oubli-numerique-mieux-proteger-les-donnees-personnelles-des-interna.

l'existence de ce droit. Adoptant une approche pragmatique, les juges parisiens ont considéré avec sérieux les incidences et les évolutions qui s'imposent au regard de l'omniprésence, dans la société contemporaine, des nouvelles technologies et en particulier de l'internet et des dangers accrus de conservation des données nominatives qui en résultent : « *si l'oubli procédait jadis des faiblesses de la mémoire humaine, de sorte qu'il n'y avait pas à consacrer un " droit à l'oubli ", la nature y pourvoyant, la société numérique, la libre accessibilité des informations sur internet, et les capacités sans limites des moteurs de recherche changent considérablement la donne et justifient pleinement qu'un tel droit soit aujourd'hui revendiqué, non comme un privilège qui s'opposerait à la liberté d'information, mais comme un droit humain élémentaire à l'heure de la société de conservation et d'archivage numérique sans limite de toute donnée personnelle et de l'accessibilité immédiate et globalisée à l'information qui caractérisent les technologies contemporaines et la fascinante insouciance qu'elles suscitent* » [638]. Parallèlement, à l'issue d'un rapport rendu public le 27 mai 2009, une proposition sénatoriale préconise de « *réfléchir à la création* […] *d'un droit à l'oubli* » [639]. S'inspirant de cette recommandation, la proposition de loi du 6 novembre 2009 [640] envisage de modifier la loi IFL en permettant notamment de rendre plus effectif l'exercice de ce droit à travers plusieurs mesures. La proposition sénatoriale prévoit une obligation pour la CNIL de préciser dans la liste des traitements de données qu'elle met à disposition du public, la durée de conservation des données et ce, pour chacun des types de traitements y figurant [641]. Quant au responsable du traitement, ce dernier serait tenu de fournir aux internautes « *une information claire, accessible et spécifique* » sur la durée de conservation de leurs données et la possibilité pour la personne concernée d'exercer ses droits d'accès, de suppression et de rectification [642]. Par ailleurs, le droit d'opposition visé à l'article 38 de la loi de 2004 tel que préconisé par la proposition de loi de 2009 encourage la consécration d'une forme d'oubli. En définitive, comme l'observe le professeur Jean FRAYSSINET, « *l'intention d'établir ce qui commence à ressembler à un vrai droit à l'oubli est là et elle correspond à la montée d'une demande sociale engendrée par des problèmes sociaux apparus spécialement dans le cadre de l'internet* » [643]. L'éventuel vote de la loi permettra de connaître avec plus de certitude la teneur de ce droit. Dans l'attente, il est d'ores et déjà important de rappeler que la donnée la plus facile à protéger reste celle qui n'a jamais

[638] TGI Paris, ord. réf. 25 juin 2009, *Vernes c/* SAS *Les Échos*, jugement préc.
[639] Yves DETRAIGNE et Anne-Marie ESCOFFIER (présenté par), *Rapport d'information relatif au respect de la vie privée à l'heure des mémoires numériques*, 27 mai 2009, Doc. Sénat n° 441, spéc. recommandation n° 14, p. 107 et s., disponible sur : http://www.senat.fr/rap/r08-441/r08-4411.pdf.
[640] Proposition de loi, 6 nov. 2009, préc. – Sur ce projet de loi, v. Alain BENSOUSSAN, « Le " droit à l'oubli " sur Internet », art. préc.
[641] Art. 5 proposition de loi, 6 nov. 2009, préc.
[642] Art. 6 proposition de loi, 6 nov. 2009, préc.
[643] Jean FAYSSINET, « Le pseudo droit à l'oubli appliqué à la presse », chron. préc., spéc. p. 180.

été divulguée sur l'internet. Dans ces conditions, il est impératif que les internautes adoptent une attitude vigilante lorsqu'ils communiquent en ligne leurs données nominatives, cette attitude impose à l'évidence un renforcement de l'éducation et de la sensibilisation de ces derniers [644].

238. Bilan. Il ressort clairement de cette étude que la pratique du *spamming* s'exerce en violation des obligations qui s'imposent à tout responsable de traitement et des droits reconnus au titulaire de données [645]. Aussi convient-il d'analyser si le volet pénal de la loi de 2004 sanctionnant les actes commis en violation de cette loi apparaît assez dissuasif pour que les « spammeurs » aient à craindre pour la poursuite de leur activité.

§ 3. LE VOLET RÉPRESSIF : UN BILAN DÉCEVANT

239. La nécessité de créer un droit pénal « spécialisé ». La facilité avec laquelle les données peuvent s'échanger et circuler sur la toile a augmenté de façon exponentielle les risques d'atteinte encourus par les données à l'occasion de leurs traitements. L'environnement technique des problématiques posées et la multiplication des comportements délictuels nouveaux ont ainsi imposé la construction d'un droit pénal sanctionnant spécifiquement les comportements commis en violation de la loi IFL [646]. Il convient dès lors d'évaluer si ce droit pénal « technique » peut prétendre constituer une réponse suffisamment pertinente face à l'agressivité du *spamming*. Il sera démontré que, malgré la détermination ferme du législateur de consolider la protection des données comme en atteste un arsenal pénal en théorie prometteur (A.), sa mise en œuvre se révèle en pratique décevante (B.).

[644] La Commission européenne, dans le cadre du projet de révision de la directive 95/46/CE, encourage une sensibilisation des internautes sur les risques encourus par leurs données nominatives lorsque celles-ci sont mises en ligne, en privilégiant l'autorégulation (*soft law*). À ce titre, elle énonce que les initiatives prises pourront, par exemple, se concrétiser sous la forme de « *campagnes de sensibilisation dans la presse écrite et les médias électroniques, la publication d'informations claires sur des sites Web qui décrivent précisément les droits des personnes concernées et les responsabilités des responsables du traitement* » (« Une approche globale de la protection des données à caractère personnel », communication préc., spéc. p. 9). – V. ég. Conseil national de la consommation, *Rapport sur la protection des données personnelles des consommateurs*, 18 mai 2010, spéc. p. 5, disponible sur : http://www.minefe.gouv.fr/directions_services/dgccrf/boccrf/2010/10_06/rapport_CNCdonnees_personnelles.pdf.

[645] CNIL, *Rapport d'activité 2002*, rapport préc., spéc. pp. 48-52.

[646] Jean FRAYSSINET le définit comme un « *droit pénal spécialisé* » au sein du droit pénal spécial constituant « *une forme exemplaire de droit pénal technique* » (*Informatique fichiers et Libertés*, *op. cit.*, spéc. n° 228, p. 98). – Cette tendance accrue à rendre le droit pénal spécial de plus en plus spécifique et technique se retrouve notamment dans le domaine de la bioéthique, v. par ex. Agathe LEPAGE, « Loi du 6 août 2004. Réflexions de droit pénal sur la loi du 6 août 2004 relative à la protection des personnes à l'égard des traitements de données à caractère personnel », *Comm. com. électr.* févr. 2005, Étude 9, p. 33 et s, spéc. n° 20, p. 36).

A. UN ARSENAL PENAL PROMETTEUR EN THEORIE

240. Souhaitant faire du volet pénal un instrument de répression effectif, garant du respect de la loi IFL et de la protection des droits des titulaires de données, le législateur de 2004 a renforcé d'une part la sévérité des textes (1.) et d'autre part les pouvoirs de la CNIL (2.).

1. Une sévérité accrue dans les textes

241. L'article 50 de loi de 2004 dispose que « *les infractions aux dispositions de la présente loi sont prévues et réprimées par les articles 226-16 à 226-24 du Code pénal* ». À la lecture de cette disposition, il semblerait de prime abord que cette loi n'apparaît pas innover en la matière, les textes pénaux qui y sont visés étant les mêmes que ceux contenus dans l'ancienne loi de 1978 [647]. Cependant, face à l'ampleur des dangers qu'encourent les données, le législateur de 2004 a souhaité renforcer en amont le dispositif pénal par la multiplication des textes d'incrimination (a.) et en aval, par l'aggravation des sanctions fixées (b.).

a. La multiplication des textes d'incrimination

242. Pour les besoins de notre recherche, nous nous appuierons sur les exemples les plus marquants afin de mettre en évidence les évolutions qui ont eu lieu. Pour cela, seules les dispositions susceptibles de concerner la pratique du *spamming* seront étudiées [648].

243. Le maintien des incriminations antérieures. La grande majorité des comportements poursuivis aujourd'hui au titre des articles 226-16 et suivants du Code pénal

[647] Sur le dispositif répressif accompagnant la loi de 1978, v. not. André LUCAS, Jean DEVEZE, Jean FRAYSSINET *Droit de l'informatique et de l'Internet*, *ibid.*, spéc. n° 948, p. 669.

[648] Ne seront pas mentionnés dans les prochains développements les articles suivants : le nouvel article 226-16-1 du Code pénal qui sanctionne l'utilisation sans autorisation du numéro d'inscription des personnes au répertoire national d'identification des personnes physiques, l'article 226-19 du même code qui interdit de mettre ou conserver en mémoire informatisée, sans le consentement de l'intéressé, les données dites sensibles et enfin, le nouvel article 226-19-1 du même code relatif au traitement de données à caractère personnel ayant pour fin la recherche dans le domaine de la santé.

procède de la conservation dans la nouvelle loi des incriminations préexistantes [649]. Ce maintien est d'emblée attesté par le fait que la réforme a conservé en tête de cette série d'infractions, le délit qui consiste dans le fait « *y compris par négligence, de procéder ou de faire procéder à des traitements de données à caractère personnel sans qu'aient été respectées les formalités préalables à leur mise en œuvre* » [650]. De façon générale, les comportements commis en infraction aux principes et aux règles de protection fixées par la loi IFL sont sanctionnés par les dispositions du Code pénal [651], à savoir le non-respect des formalités préalables à la mise en œuvre d'un traitement automatisé [652], la violation des obligations en matière de sécurité [653], en matière de collecte [654], de conservation des données [655], le non-respect du droit d'opposition [656], la divulgation de données sans autorisation [657] ou le détournement de la finalité du traitement [658] ou des règles régissant le transfert de données vers un État n'appartenant pas à l'Union européenne [659].

[649] Il convient toutefois de noter que certains articles ont été remodelés en scindant une disposition pour en faire plusieurs textes. Tel est le cas par exemple de l'article 226-18 du Code pénal qui se décompose aujourd'hui en deux articles distincts. L'article 226-18 nouveau du Code pénal sanctionne toujours « *le fait de collecter des données à caractère personnel par un moyen frauduleux, déloyal ou illicite* ». Mais le non-respect de l'opposition initialement visée à l'alinéa 1er de l'article 226-18 susvisé est transféré dans le nouvel article 226-18-1 qui incrime « *le fait de procéder à un traitement de données à caractère personnel concernant une personne physique malgré l'opposition de cette personne, lorsque ce traitement répond à des fins de prospection, notamment commerciale, ou, lorsque cette opposition est fondée sur des motifs légitimes* ».

[650] Art. 226-16 C. pén. – V. par ex. CA Aix-en-Provence, 9 oct. 2001, *Juris-Data* n° 2001-170316 (condamnation à deux d'emprisonnement avec sursis). – CA Toulouse, 3e ch. corr., 12 juin 2005, *Juris-Data* n° 2005-272643 (condamnation à 5.000 euros d'amende).

[651] Pour une étude détaillée de l'ensemble de ces infractions, v. Jean FRAYSSINET, *Atteintes aux droits de la personne résultant des fichiers ou des traitements informatiques*, fasc. préc., spéc. n° 93 et s. – À noter qu'il existe également, outre les délits prévus et réprimés aux articles 226-16 et suivants du Code pénal, des contraventions fixées aux articles R. 625-10 à R. 625-12 C. pén. : en cas de défaut d'information (art. R. 625-10 C. pén.), en l'absence de réponse du responsable à une demande du titulaire des données (art. R. 625-11 C. pén.) ou lorsque le responsable du traitement ne procède pas, sans frais pour le demandeur, à la rectification, la mise à jour ou la suppression des données concernant ce dernier (art. R. 625-12 C. pén.).

[652] V. par ex. Cass. crim. 30 oct. 2001, pourvoi n° 99-82136, *inédit* (condamnation à 50.000 euros et 30.000 euros de deux dirigeants d'un syndicat de médecins du travail pour avoir mis en œuvre un système de traitement automatisé des dossiers médicaux sans avoir procédé au préalable à sa déclaration auprès de la CNIL). – En matière de *spamming*, v. TGI Paris, 6 juin 2003, *Ministère public et M. Thomas Quinot c/ M. R.G.U.*

[653] Art. 226-17 C. pén. – V. par ex. Cass. crim. 30 oct. 2001, arrêt préc. (condamnation des dirigeants d'un syndicat de médecins du travail pour ne pas avoir pris toutes les mesures destinées à empêcher à des tiers non autorisés l'accès aux dossiers médicaux).

[654] Art. 226-18 C. pén. – V. par ex. Cass. crim. 28 sept. 2004, pourvoi n° 03-86604, *Bull. crim*, n° 224, p. 801 (ont été respectivement condamné à 5.000 euros d'amende avec sursis le président d'une association et cette association pour traitement de données nominatives malgré l'opposition d'un ancien membre qui avait demandé à ne plus figurer dans les fichiers). – CA Toulouse, 3e ch. corr., 12 juin 2005, arrêt préc. (condamnation à 3.000 euros d'amende pour non-respect du droit d'opposition). – TGI Paris, 31e ch., 18 sept. 2008, *Éditions Neressis c/ Arkadia, Stéphane V. C.*, jugement préc. (condamnation à 5.000 euros d'amende pour la collecte déloyale de données mais également pour d'autres infractions). – En matière de *spamming*, v. Cass. crim. 14 mars 2006, arrêt préc. (condamnation à 3.000 euros d'amende pour collecte déloyale).

[655] Art. 226-20 C. pén.

[656] Art. 226-18-1 C. pén.

[657] Art. 226-22 C. pén. – Pour un exemple de condamnation sur ce fondement, v. CA Paris, 9e ch. corr., sect. B, 17 sept. 2004, *Juris-Data* n° 2004-255097 (a été condamné une amende de 1.000 euros un agent immobilier pour la divulgation volontaire et sans autorisation de données nominatives susceptibles de porter atteinte à la vie privée ou à la considération).

244. La création de nouvelles incriminations. Outre les infractions antérieures à la réforme de 2004 qui sont restées presque inchangées, certains articles ont été créés et correspondent à de véritables innovations à l'origine de nouvelles incriminations. Tel est le cas par exemple de l'article 226-16-1-A du Code pénal qui a instauré une nouvelle infraction en incriminant le fait de ne pas respecter, y compris par négligence, les normes simplifiées ou d'exonération fixées par la CNIL à l'occasion d'un traitement de données à caractère personnel [660]. De même, parmi ces innovations figure également l'article 226-22-1 du Code pénal qui sanctionne le transfert de données à caractère personnel faisant l'objet d'un traitement vers un État n'appartenant pas à la Communauté européenne opéré en violation des mesures prises par la CNIL ou encore l'article 226-22-2 du même code qui dispose que « *l'effacement de tout ou partie des données à caractère personnel faisant l'objet du traitement ayant donné lieu à l'infraction peut être ordonné* ». Cette inflation législative est symptomatique d'une évolution vers un « *droit pénal sanctionnateur* » [661], mouvement qui se confirme d'ailleurs au regard de l'aggravation des sanctions fixées.

b. L'aggravation des sanctions fixées

245. La revalorisation des peines. Soucieux d'assurer aux condamnations prononcées un caractère dissuasif, le législateur a rehaussé les sanctions, s'alignant ainsi sur la position de la CNIL [662]. Ce durcissement est patent à travers le *quantum* des peines découlant de l'application des articles 226-16 à 226-22-1 du Code pénal qui s'alignent désormais uniformément sur une peine de cinq ans d'emprisonnement et de 300.000 euros d'amende, comme le prévoyaient les anciennes dispositions du Code pénal pour les peines

[658] Art. 226-21 C. pén. – v. par exemple, CA Aix-en-Provence, 7e ch., sect. A, 30 juin 2009, *Juris-Data* n° 2009-014406, *Comm. com. électr.* mars 2010, comm. 27, p. 33 et s., note A. Lepage. – Pour des faits similaires, v. Cass. crim. 20 juin 2006, pourvoi n° 05-86.491, *inédit* (ont été condamnés à dix mois d'emprisonnement et à un an d'emprisonnement avec sursis deux policiers pour avoir détourné de leur finalité des données à caractère personnel contenues dans un système de traitement des infractions constatées). – Avant 2004, v. not. TGI Rennes, 8 déc. 1988, *Expertises* 1989, n° 115, p. 104 et s., note J. Frayssinet (s'est rendue coupable de ce délit une Caisse d'épargne pour avoir utilisé des données à caractère personnel de ses clients pour des finalités autres que celle pour laquelle elles avaient l'objet d'une déclaration simplifiée). – TGI Paris 17e ch. corr., 16 déc. 1994, *Juris-Data* n° 1994-600554 ; *Expertises* 1995, n° 181, p. 120, note J. Sanqueur. – V. ég. Michel VIVANT et Christian LE STANC, « Droit de l'informatique », *JCP* 1995, éd. E., I. 461, spéc. n° 17.

[659] Art. 226-22-1 C. pén.

[660] Sur ces normes simplifiées ou les dispenses de déclaration, v. le site de la CNIL disponible sur : http://www.cnil.fr/en-savoir-plus/deliberations/normes-simplifiees/ et http://www.cnil.fr/en-savoir-plus/deliberations/dispenses-de-declaration/.

[661] Agathe LEPAGE, « Réflexions de droit pénal sur la loi du 6 août 2004 relative à la protection des personnes à l'égard des traitements de données à caractère personnel », chron. préc., spéc. n° 14, p.35.

[662] La CNIL estimait que « *l'abaissement des sanctions qui s'attache à la méconnaissance de la loi,* […] *ne paraît pas justifié. Une telle initiative pourrait de surcroît altérer l'esprit de la réforme : la protection des données personnelles et de la vie privée n'a pas une moindre valeur aujourd'hui qu'hier* » (Avis sur le projet de loi modifiant la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, 26 septembre 2000, spéc. p. 11, disponible sur : http://www.cnil.fr/fileadmin/documents/approfondir/textes/aviscnildonneesperso.pdf).

les plus fortes [663]. Les sanctions prévues pour la divulgation des données sans le consentement de l'intéressé sont particulièrement révélatrices de cette tendance vers une plus grande sévérité : alors que la peine ne s'élevait qu'à un an d'emprisonnement sous l'empire de l'ancienne loi, ce comportement est désormais puni de cinq ans d'emprisonnement et de 300.000 euros d'amende [664]. La seule exception à l'uniformisation des sanctions est l'incrimination de divulgation de données par imprudence ou négligence qui est portée à trois ans d'emprisonnement et à 100.000 euros d'amende contre 7.500 euros avant 2004 [665], ce qui reste malgré tout très élevé.

246. La remise en cause de la pertinence des sanctions. Si l'aggravation des peines est justifiée par la volonté de garantir une meilleure protection des données par un effet dissuasif, il convient de s'interroger sur l'opportunité d'une telle sévérité. En effet, l'uniformisation des peines revient à placer sur un même pied d'égalité toutes les infractions alors que chacune d'elles présente un degré de gravité distinct. En particulier, il semble que les sanctions prévues pour le non-respect des formalités préalables à la mise en œuvre d'un traitement de données (5 ans d'emprisonnement et 300.000 euros) apparaissent excessives dès lors que ce manquement est dû à une simple négligence [666]. Le caractère disproportionné des peines fixées est révélateur du décalage qui existe entre le contenu des textes et la nécessité de sanctionner les comportements illicites. Un tel décalage est regrettable puisqu'il conduit à constater le détachement de l'œuvre législative aux réalités pratiques.

[663] Avant la réforme de 2004, les sanctions variaient en fonction des infractions considérées. Des peines plus sévères coexistaient ainsi avec d'autres plus faibles : par exemple, le non-respect des formalités préalables à leur mise en œuvre d'un traitement automatisé d'informations nominatives (art. 226-16 ancien) et le traitement ou la conservation de ces informations au-delà de la durée prévue par la demande d'avis ou la déclaration préalable à la mise en œuvre du traitement (art. 226-20 ancien) étaient punis de trois ans d'emprisonnement et de 45.000 euros d'amende.

[664] Art. 226-22, al. 1er C. pén.

[665] Art. 226-22, al. 2 C. pén.

[666] Guy BRAYBANT, Conseiller d'État, favorable à un assouplissement de la répression, recommandait à l'occasion de la transposition de la directive de 1995, de tenir compte du degré de gravité des infractions et de distinguer ainsi « *selon que le comportement en cause est manifestement destiné à porter atteinte à la liberté ou qu'il révèle seulement une violation d'une règle de forme* […], *le premier étant toujours puni d'une peine correctionnelle – dont le quantum ne saurait dépasser trois ans – le second, d'une peine contraventionnelle* » (*Données personnelles et société de l'information*, rapport préc., spéc. p. 120). – De même, Agathe LEPAGE reproche ce « *manque de pondération* », clairement attesté au regard des différences très nettes entre les sanctions prévues en cas d'atteintes à la vie privée ou à l'honneur et celles fixées pour les infractions en matière de traitement des données à caractère personnel alors même que les valeurs protégées sont identiques (« Réflexions de droit pénal sur la loi du 6 août 2004 relative à la protection des personnes à l'égard des traitements de données à caractère personnel », chron. préc., spéc. nos 28 à 30, pp. 38-39). – Jean FRAYSSINET est également favorable à un abaissement du *quantum* des peines par la prise en compte des particularités de chacune des infractions, notamment au regard de leur degré de gravité (« La régulation du respect de la loi Informatique, fichiers et libertés par le droit pénal : une épée en bois », *Legicom* 2009/1, n° 42., p. 23 et s., spéc. pp. 28-29).

2. Le renforcement des pouvoirs de la CNIL

247. Le durcissement des pouvoirs de la CNIL : de l'avertissement à la sanction. Sous la loi de 1978, les pouvoirs de la CNIL se bornaient à émettre un avertissement et à dénoncer au Parquet les infractions à la loi IFL dont elle avait connaissance, lequel jugeait alors de l'opportunité des poursuites [667]. Cette dernière hypothèse a été notamment mise en œuvre suite à sa célèbre opération « Boîte à *spams* », à l'issue de laquelle cinq dossiers avaient été transmis au Parquet [668]. Par ailleurs, bien qu'investie d'un pouvoir d'enquête dès lors qu'un traitement est suspecté d'être contraire aux obligations de la loi IFL [669], la Commission ne disposait d'aucun moyen de contrainte pour rendre effectives ses investigations. Conscient d'une certaine paralysie de la Commission, le législateur de 2004 est intervenu en renforçant ses pouvoirs d'action, lui permettant d'exercer un contrôle sur la conformité des systèmes de traitements de données. La CNIL s'est ainsi vue attribuer d'importantes prérogatives en matière de contrôle *a posteriori* dans les locaux professionnels [670]. En cas de violation de la loi IFL et selon la gravité des manquements commis, la Commission peut prononcer un avertissement et mettre en demeure le responsable du traitement de faire cesser tout agissement réalisé en violation des dispositions de la loi IFL [671]. En cas d'urgence, lorsque la mise en œuvre d'un traitement ou l'exploitation des données traitées entraîne une violation de l'identité humaine, des droits de l'homme, de la vie privée, ou des libertés individuelles ou publiques visées à l'article 1er de la loi de 2004, elle peut notamment, après une procédure contradictoire, décider d'interrompre la mise en œuvre du traitement ou verrouiller certaines des données à caractère personnel traitées et ce, pour une durée maximale de trois mois [672]. En, cas d'atteinte grave aux droits et libertés précédemment énumérés, elle pourra demander en référé toute mesure de sécurité

---

[667] Art. 21, 4° loi n° 78-17.

[668] Sur cette opération et les poursuites engagées contre l'une des cinq sociétés mises en causes, v. *supra* : n° 200.

[669] Art. 21, 2° loi n° 78-17 et art. 44 loi n° 2004-801. – Suite aux plaintes adressées à la CNIL, cette dernière interroge le responsable du traitement mis en cause afin d'obtenir des précisions quant à la mise en œuvre du traitement opéré. Selon les informations communiquées par la personne interrogée, si la Commission estime que les réponses apportées sont imprécises ou semblent inexactes, elle procèdera à une mission de contrôle sur place, dans les locaux du responsable, afin de vérifier la conformité de ses déclarations au traitement réellement pratiqué. Depuis juin 2010, les plaintes peuvent être adressées à la CNIL par voie électronique (v. CNIL, « Vous souhaitez supprimer vos données sur internet : ayez le réflexe « plainte en ligne » ! », actualité, 24 nov. 2010, disponible sur : http://www.cnil.fr/dossiers/conso-pub-spam/actualites/article/vous-souhaitez-supprimer-vos-donnees-personnelles-sur-internet-ayez-le-reflexe-plainte-en-l/).

[670] Art. 44 loi n° 2004-801. – L'article 62 D. n° 2005-1309 du 20 octobre 2005 préc. précise que « *lorsque la commission effectue un contrôle sur place, elle informe au plus tard au début du contrôle le responsable des lieux de l'objet des vérifications qu'elle compte entreprendre, ainsi que de l'identité et de la qualité des personnes chargées du contrôle* ». – V. not. CE, sect. contentieux, 6 nov. 2009, n° 304300, *Sté Inter Confort*, *Juris-Data* n° 2009-012926, *Comm. com. électr.* févr. 2010, p. 42 et s., note É. A. Caprioli (jugeant que la seule mention faite à ce responsable que le contrôle est exercé en application de l'article 44 précité est insuffisante pour respecter l'exigence d'information requise).

[671] Art. 45 I loi n° 2004-801.

[672] Art. 45 II, 1° et 2° loi n° 2004-801.

nécessaire à la sauvegarde de ces droits et libertés [673]. Surtout, l'entrée en vigueur de la loi du 6 août 2004 a marqué un tournant décisif pour la CNIL puisqu'après trente années d'existence, cette dernière se voit dotée d'un pouvoir de sanction, y compris pécuniaire [674], par une décision motivée et après une procédure contradictoire [675], ce qui lui permet désormais d'asseoir son autorité.

248. Mise en œuvre du pouvoir de sanction. Si au terme du délai fixé par la Commission, délai octroyé au responsable du traitement pour lui permettre de se conformer à la mise en demeure, elle constate que le comportement de ce dernier n'a pas évolué, elle rédigera un rapport sur la base duquel elle s'appuiera pour décider du prononcé d'une éventuelle sanction. Ce rapport joue un rôle important puisqu'il contient une proposition de sanction à l'encontre du responsable du traitement [676]. À l'issue d'une confrontation des arguments avancés par le responsable du traitement aux reproches établis dans le rapport, la Commission décidera de prononcer une sanction si elle conclut au non-respect de la mise en demeure [677]. Le montant de cette sanction ne peut excéder 150.000 euros à l'occasion de la constatation d'un premier manquement [678]. En revanche, en cas de récidive dans les cinq ans suivant la date à laquelle la sanction pécuniaire prononcée est devenue définitive, le montant pourra être porté jusqu'à 300.000 euros, sans excéder 5 % du chiffre d'affaires hors taxes lorsque la personne condamnée est une entreprise [679]. En tout état de cause, le montant de la sanction doit être proportionné à la gravité du manquement commis et aux avantages tirés de ce dernier [680]. De surcroît, lors de l'exercice de sa mission, aucune entrave ne peut lui être opposée, y compris le secret professionnel, sous peine de sanctions qui peuvent atteindre 150.000 euros. Enfin, la CNIL peut, « *en cas de mauvaise foi* » du responsable du traitement mis en cause, ordonner la publication des sanctions qu'elle prononce dans un journal par

[673] Art. 45 III loi n° 2004-801.
[674] Art. 45 à 48 loi n° 2004-801. – Ce n'est qu'à partir de 2006 que la Commission met en œuvre ce pouvoir à l'encontre de onze entreprises dont l'activité violait les obligations de la loi de 2004, sanctions dont le montant total s'élevait à 168.300 euros (v. en ce sens, CNIL *Rapport d'activité 2006*, n° 27, Doc. fr., 2007, spéc. p. 23). – Sur le rôle et les pouvoirs de la CNIL, v. not. David FOREST, « Trente ans et des poussières. Retour sur les premiers pas de la CNIL », *RLDI* janv. 2008, n° 1159, p. 77 et s. – Romain PERRAY, « Quel avenir pour le pouvoir de sanction de la CNIL ? », *RLDI* janv. 2008, n° 1160, p. 82 et s.
[675] Art. 45 I, 1° loi n° 2004-801.
[676] Art. 46, al. 1er loi n° 2004-801. – En réponse à ce rapport, le responsable peut, représenté ou assisté de son conseil, produire un mémoire en défense. Cet écrit sera exposé oralement devant la formation restreinte de la CNIL et lui permettra de se justifier eu égard aux reproches formulés (*Id*.).
[677] Art. 45 I loi n° 2004-801.
[678] Art. 47, al. 2 loi n° 2004-801.
[679] Art. 47, al. 3 loi n° 2004-801.
[680] Art. 47, al. 1er loi n° 2004-801.

exemple [681], cette mesure est une sanction lourde dans la mesure où elle peut engendrer des conséquences irréversibles en termes d'image et de réputation pour la société condamnée [682].

249. Le renforcement du caractère juridictionnel de la CNIL : une initiative pertinente. Toute violation des dispositions de la loi IFL peut être poursuivie devant les juridictions répressives ou devant la CNIL, garante du respect de cette législation [683]. À ce titre, le Conseil d'État a énoncé en 2008 que, « *eu égard à* [la nature de la CNIL], *sa composition et ses attributions,* [celle-ci] *peut-être qualifié*[e] *de tribunal au sens de l'article 6-1 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales* [qui consacre le droit à un procès équitable] » [684]. Au regard des règles relatives au procès équitable, plusieurs conséquences procédurales en résultent. Tout d'abord, cette qualification emporte nécessairement l'obligation pour la Commission d'agir comme un tribunal indépendant et impartial. Par ailleurs, la procédure doit être contradictoire et les audiences ainsi que les décisions prononcées doivent être publiques. Or, si la procédure suivie devant la formation restreinte [685] est contradictoire [686], ni ses audiences ni les décisions rendues (mises en demeure, avertissements et sanctions financières) ne sont pas, par principe, publiques sauf à la demande des parties. Si les audiences sont publiques, elles ne doivent pas porter atteinte à l'ordre public, à la protection de la vie privée de l'une des parties concernées ou au secret des affaires ou à tout autre secret protégé par la loi [687]. Quant à la publicité des décisions, celle-ci est également possible en cas de « *mauvaise foi* » du responsable du traitement mais à la seule discrétion de la Commission [688]. Afin de tirer toutes les conséquences de son rôle juridictionnel [689], le Sénat propose la publicité systématique des audiences de la formation restreinte [690] mais aussi celle des sanctions les plus graves prononcées par la Commission en supprimant la condition de mauvaise foi afin d'étendre le champ de diffusion de ses décisions [691]. Cette modification est opportune car elle

[681] Art. 46, al. 2 loi n° 2004-801.
[682] Comme le reconnaît Philippe NOGRIX, rapporteur en formation restreinte dans le dossier du Crédit Lyonnais, « *il est indéniable que le risque d'image et le risque juridique liés à l'exploitation de données personnelles sont plus importants qu'ils ne l'étaient hier* » (CNIL, *Rapport d'activité* 2006, rapport préc., spéc. p. 24).
[683] Romain PERRAY, « Quel avenir pour le pouvoir de sanction de la CNIL ? », art. préc.
[684] CE, ord. réf., sect. contentieux, 19 févr. 2008, réq. n° 31194, *Profil France*, *Juris-Data* n° 2008-073370. – V. déjà en ce sens, Conseil d'État, *Les autorités administratives indépendantes,* Doc. fr., coll. *Études et Documents,* n° 52, 2001, spéc. p. 360.
[685] Art. 17 loi n° 2004-801 : « *La formation restreinte de la commission prononce les mesures prévues au I et au 1° du II de l'article 45* [avertissent, mise en demeure, sanction pécuniaire, injonction de cessation des agissements illicites] ».
[686] Art. 45-I loi n° 2004-801.
[687] Art. 16 délibération n° 2006-147 du 23 mai 2003 fixant le règlement intérieur de la CNIL, J.O. du 7 juillet 2006, n° 156.
[688] Art. 46, al. 2 loi n° 2004-801.
[689] CE, ord. réf., sect. contentieux, 19 févr. 2008, arrêt préc.
[690] Art. 10 de la proposition de loi, 6 nov. 2009, préc.
[691] Art. 11 de la proposition de loi, 6 nov. 2009, préc.

constituerait une mesure « *efficace et dissuasive* » à l'encontre des responsables de traitement ayant violé la loi IFL [692]. Enfin, la proposition de loi de 2009 tend à ajouter au titre des compétences de la CNIL la possibilité d'exposer, d'office ou à la demande des parties des observations devant les juridictions est particulièrement intéressante. Ainsi, outre la possibilité pour la CNIL de transmettre au procureur de la République les infractions dont elle a connaissance et de répondre à des demandes d'avis des juridictions [693], l'article 13 de la proposition de loi précitée ajouterait au titre des compétences de la Commission la possibilité pour celle-ci d'avoir une réelle influence sur la décision des juridictions d'autant plus forte que ces dernières ne pourraient frapper ses observations d'irrecevabilité, quand même s'il s'agirait d'une procédure orale.

B. UNE MISE EN ŒUVRE DECEVANTE EN PRATIQUE

250. Si le législateur démontre une réelle détermination à la mise en place d'un dispositif pénal efficace et dissuasif, cette volonté est largement déçue dès lors que l'on s'attache en pratique à ses effets. Les imperfections rédactionnelles dont souffre ce dispositif sont source d'insécurité juridique (1.). Par ailleurs, il apparaît que ces textes sont peu sollicités, la violation de la loi IFL ne suscitant qu'un contentieux rare qui aboutit le plus souvent à de faibles sanctions (2.). Enfin, ce décalage entre la théorie et la pratique se vérifie également au regard de l'intervention de la CNIL puisque malgré le renforcement de ses pouvoirs, et notamment son pouvoir de sanction [694], la Commission se révèle être une main-forte insuffisante à la loi pénale (3.).

1. Les imperfections rédactionnelles de la loi pénale, source d'insécurité juridique

251. Le volet répressif de la loi de 2004 n'est pertinent que s'il est garant du respect de la loi. Sans entrer dans une analyse détaillée de l'ensemble des dispositions pénales – là n'est pas notre propos – la sélection des exemples les plus probants conduiront à dénoncer, à l'instar du professeur Jean FRAYSSINET, les défauts rédactionnels de cette

[692] Yves DETRAIGNE et Anne-Marie ESCOFFIER (présenté par), *Rapport d'information relatif au respect de la vie privée à l'heure des mémoires numériques*, rapport préc. spéc. p. 88.
[693] Art. 40, al. 2 C. procédure pénale. – Art. 49 délibération n° 2006-147 préc.
[694] On retrouve ce même décalage à propos de son pouvoir de contrôle qui, malgré son renforcement par la loi de 2004, a été largement freiné et paralysé par le Conseil d'État (v. en ce sens, CE, sect. contentieux, 6 nov. 2009, arrêt préc.)

législation [695]. L'absence de clarté et de lisibilité qu'ils induisent est source d'incertitude et plus gravement, d'insécurité juridique.

252. Un manque de clarté. Certainement dans un souci d'alléger les textes, le législateur a réduit certains articles du Code pénal à leur plus simple appareil en procédant par renvoi substantiel aux dispositions de la loi de 2004. Si cette technique a certes permis de ne pas tomber dans un excès de prose, elle a fait perdre en lisibilité. Tel est le cas par exemple de l'article 226-16, alinéa 2 du Code pénal qui sanctionne « *le fait, y compris par négligence, de procéder ou de faire procéder à un traitement qui a fait l'objet de l'une des mesures prévues au 2° du I de l'article 45 de la loi n° 78 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés* ». La première lecture de cette disposition suscite perplexité. En effet, sauf à avoir en mémoire les dispositions de la loi IFL, sa compréhension immédiate apparaît compromise et contraint à revenir à la lettre des textes pour en saisir le sens [696]. Outre l'inconvénient pratique majeur que pose la technique du renvoi, son opacité entrave de façon plus préoccupante encore la compréhension de la loi pénale et indirectement sa mise en œuvre [697].

253. Une articulation maladroite des textes. Prenons pour exemple la comparaison des articles 226-18 du Code pénal et 6, 1°) de la loi de 2004 est éloquente. Tandis que le premier texte est la reprise exacte des termes de l'article 25 de la loi de 1978 qui prohibait « *la collecte de données opérée par tout moyen frauduleux, déloyal ou illicite* », le second dispose qu'« [u]*n traitement ne peut porter que sur des données à caractère personnel qui* […] *sont collectées et traitées de manière loyale et licite* ». La lecture de ces dispositions laisse apparaître plusieurs divergences rédactionnelles. D'une part, la notion de « *traitement* » figurant dans la loi de 2004 n'est pas reprise à l'article 226-18 du Code pénal, et d'autre part, le terme « *frauduleux* », visé dans le Code pénal, est absent de la loi de 2004.

[695] Pour une étude approfondie des multiples « *malfaçons* » que recèle ce dispositif pénal, v. Jean FRAYSSINET, « La régulation du respect de la loi Informatique, fichiers et libertés par le droit pénal : une épée en bois », chron. préc., spéc. pp. 25-27).

[696] Le recours à cette technique est d'autant plus regrettable que certaines dispositions pénales rédigées sous l'empire de la loi de 1978 étaient plus claires. Tel est le cas par exemple de l'article 226-17 du Code pénal qui réprimait « *le fait de procéder ou de faire procéder à un traitement automatisé d'informations nominatives sans prendre toutes les précautions utiles pour préserver la sécurité de ces informations et notamment empêcher qu'elles ne soient déformées, endommagées ou communiquées à des tiers non autorisés* ». Si cette disposition figure toujours dans la loi de 2004, elle se trouve amputée d'une partie de son contenu qui participait pourtant à sa compréhension. L'article 226-17 du Code pénal est désormais rédigé ainsi : « *le fait de procéder ou de faire procéder à un traitement de données personnelles sans mettre en oeuvre les mesures prescrites à l'article 34 de la loi n° 78-17 du 6 janvier 1978* », l'article 34 disposant que le responsable du traitement doit prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès.

[697] Sur ce point, v. Agathe LEPAGE, « Réflexions de droit pénal sur la loi du 6 août 2004 relative à la protection des personnes à l'égard des traitements de données à caractère personnel », chron. préc.

Ces incohérences risquent d'accentuer les désaccords non seulement entre le juge pénal et la CNIL mais aussi au sein même de la juridiction pénale [698]. Les maladresses dans la combinaison de la loi de 2004 avec le Code pénal contribuent à alimenter les incertitudes quant à leur interprétation et rendent ainsi malaisées leur compréhension et leur application respectives.

254. Des notions mal définies, facteur de flottements jurisprudentiels. Une affaire en matière de *spamming* évoquée précédemment illustre les conséquences qui peuvent découler du manque de rigueur des textes. En l'espèce, la poursuite d'un « spammeur » sur le fondement de l'article 226-18 du Code pénal qui incrimine le fait de collecter des données par tout moyen frauduleux, déloyal ou illicite, imposait de s'interroger sur le point de savoir si l'utilisation d'adresses électroniques à des fins d'envois de *spams* caractérisait un acte de collecte au sens de la loi alors même que ces adresses n'avaient fait l'objet d'aucun enregistrement. Alors que les juges de première instance avaient refusé de qualifier cette opération de collecte [699], la Cour de cassation s'était clairement prononcée en sens contraire [700]. Cet arrêt permettait ainsi de mettre fin à une définition restrictive de la notion de collecte et de respecter le principe de l'interprétation stricte de la loi pénale, l'article 226-18 du Code pénal n'ayant « *jamais lié l'existence de l'infraction à un enregistrement ou une conservation effective* » [701].

2. Un contentieux rare et faiblement sanctionné

[698] Sur ce point, v. Jean FRAYSSINET, « La régulation du respect de la loi Informatique, fichiers et libertés par le droit pénal : une épée en bois », chron. préc., spéc. pp. 29-31. – À titre d'exemple de divergences entre les juges et la CNIL, on peut citer le célèbre débat qui a opposé la cour d'appel de Paris à la CNIL sur la question de savoir si l'adresse IP constitue une donnée à caractère personnel (pour plus de détails sur ce débat, v. *supra* : n° 187).
[699] TGI Paris, 17e ch., 7 déc. 2004, jugement préc.
[700] V. en ce sens Cass. crim., 14 mars 2006, arrêt préc.
[701] Jean FRAYSSINET, *Atteintes aux droits de la personne résultant des fichiers ou des traitements informatiques*, fasc. préc., spéc. n° 264. – En ce sens, Agathe LEPAGE observe qu'« [e]*n revenant à une lecture de l'article 226-18 davantage conforme à sa lettre et son esprit, la Cour de cassation donne des gages à une application plus sévère des dispositions pénales Informatique et libertés* » (note sous Cass. crim. 14 mars, 2006, arrêt préc., *Comm. com. électr*. sept. 2006, comm. 131, p. 43 et s.). – De même, sur les incertitudes entourant la question de l'application des dispositions pénales aux fichiers manuels, v. Jean FRAYSSINET, *Atteintes aux droits de la personne résultant des fichiers ou des traitements informatiques*, fasc. préc., spéc. n°s 81-89 (proposant ainsi de remplacer l'expression « *fichiers ou des traitements informatique* » contenue dans l'intitulé de la section V du Code pénal par la notion de « traitement ». Le « *lien d'interdépendance* » qui existe entre la loi de 2004 et le Code pénal (art. 50 loi n° 2004-801) permettrait ainsi de lever toute ambiguïté dans la mesure où la notion de « traitement » serait interprétée à la lumière de la loi IFL qui s'applique à la fois aux traitements automatisés et non automatisés (art. 2 al. 1er loi n° 2004-801)).

255. La rareté du contentieux suscité. Si le volet pénal de la loi de 2004 n'a pas engendré une littérature juridique abondante [702], le contentieux « *reste* [aussi] *quantitativement à un niveau ridiculement faible* » [703]. Ce constat est confirmé par les très rares décisions qui ont sanctionné le *spamming* pour infraction aux obligations découlant de l'application de la loi IFL [704]. À l'évidence, la mise en œuvre du dispositif souffre d'un manque d'effectivité certain qui laisse craindre que les traitements illicites se poursuivent, voire s'intensifient, faute de condamnation. Cette rareté du contentieux nous conduit à supposer que l'une des causes de ce constat découle de la méconnaissance de la législation informatique, fichiers et libertés et du manque de sensibilisation de l'ensemble des internautes. Une seconde raison peut résider dans le fait que les magistrats sont parfois peu sensibilisés aux enjeux de cette législation et donc naturellement peu enclins à se confronter à ce droit technique [705].

256. Des condamnations clémentes : une perte de crédibilité de la loi pénale La faiblesse des sanctions prononcées en la matière a des répercussions directes sur le comportement des délinquants. En effet, si les sanctions prévues par la loi de 2004 sont particulièrement élevées, pour ne pas dire excessives, il semble que l'objectif de dissuasion des contrevenants est loin d'être atteint. Les rares condamnations qui ont été prononcées, notamment à l'encontre des « spammeurs » ayant agi en violation de la loi IFL sont éloquentes sur ce point. Tel est le cas en effet lorsque la sanction d'un « spammeur » n'atteint que 3.000 euros d'amende pour défaut de déclaration préalable d'un fichier [706] ou en raison de la collecte déloyale de donnés [707] alors même que les articles 226-16 (pour la première infraction) et 226-18 (pour la seconde) du Code pénal fixent un *quantum* des peines pouvant s'élever jusqu'à 300.000 euros d'amende et cinq ans d'emprisonnement. À l'évidence, malgré le potentiel textuel des dispositions pénales, l'absence de crainte d'une

[702] Outre les études de Jean FRAYSSINET (« La régulation du respect de la loi Informatique, fichiers et libertés par le droit pénal : une épée en bois », chron. préc.) et celle d'Agathe LEPAGE (« Loi du 6 août 2004. Réflexions de droit pénal sur la loi du 6 août 2004 relative à la protection des personnes à l'égard des traitements de données à caractère personnel », chron. préc.), on peut citer Pierre-Alain WEILL, « État de la législation et tendances de la jurisprudence relatives à la protection des données personnelles en droit pénal français », art. préc.

[703] À ce titre, Jean FRAYSSINET évalue approximativement le contentieux pénal « *à moins d'une centaine de décisions de justice en matière délictuelle et contraventionnelle et moins encore de jugements de condamnations, souvent d'ailleurs à de faibles peines de principe…* » (« La régulation du respect de la loi Informatique, fichiers et libertés par le droit pénal : une épée en bois », chron. préc., spéc. p. 27). – Agathe LEPAGE, « Réflexions de droit pénal sur la loi du 6 août 2004 relative à la protection des personnes à l'égard des traitements de données à caractère personnel », chron. préc.). – Antérieurement, faisant ce même constat et le déplorant, v. not. Guy BRAIBANT, *Données personnelles et société de l'information*, rapport préc., spéc. p. 119 et s.

[704] Par exemple, v. TGI Paris, 6 juin 2003, *Ministère public et M. Thomas Quinot c/ M. R.G.U.*, jugement préc. (a sanctionné un « spammeur » à une amende de 3.000 euros pour non-respect des formalités préalables à la mise en œuvre d'un traitement automatisé de données à caractère personnel). – Cass. crim, 14 mars 2006, arrêt préc. (a sanctionné un « spammeur » pour la collecte déloyale de données à caractère personnel.

[705] V. ég. en ce sens, Agathe LEPAGE, note sous Cass. crim., 14 mars 2006, arrêt préc., note préc., spéc. p. 44.

[706] TGI Paris, 6 juin 2003, *Ministère public et M. Thomas Quinot c/ M. R.G.U.*, jugement préc.

[707] Cass. Crim., 14 mars 2006, arrêt préc.

réelle sanction pénale fait perdre au volet pénal tout l'effet dissuasif escompté. En effet, en mesurant les risques de sanction encourus aux enjeux et bénéfices financiers que les « spammeurs » sont susceptibles d'engranger, le dilemme est rapidement dissipé chez ces derniers.

3. La CNIL, une main-forte insuffisante à la loi pénale

257. Un pouvoir sous-exploité. Selon le dernier rapport de la CNIL, celle-ci a comptabilisé avoir reçu en 2009, 4265 plaintes pour non-respect de la loi IFL, un chiffre quasi identique à celui de l'année précédente (4.244), mais qui a doublé en dix ans avec 270 contrôles, 91 mises en demeure, cinq sanctions financières et quatre avertissements. Malgré un pouvoir de sanction, les sanctions financières prononcées par la CNIL depuis 2006 ne dépassent rarement en pratique 30.000 euros comme le révèlent les sanctions les plus récemment prononcées. Telle a été par exemple le montant de la sanction prononcée par la Commission à l'encontre de la société ISOTHERM qui, lors d'opérations de prospection commerciale par voie téléphonique, avait violé de nombreuses obligations auxquelles elle était pourtant tenue de se conformer en qualité de responsable de traitement [708]. Une peine identique avait été infligée à la société CDISCOUNT pour manquement au droit d'opposition que les abonnés avaient tenté d'exercer à plusieurs reprises pour se désabonner des listes de diffusion de cette dernière ainsi que pour manquement à l'obligation de répondre aux demandes de la CNIL [709]. En revanche, la CNIL a été moins sévère envers la société STUDIO REPLAY, « spammeuse », qui avait été condamnée à une amende de 10.000 euros pour manquement au droit d'opposition, à l'obligation d'accomplir les formalités préalables à la mise en œuvre de traitements ainsi que pour son absence de réponse aux demandes de la CNIL [710]. La société NEUF-CLUB INTERNET avait pour sa part été condamnée par la CNIL à une amende de 7.000 euros pour violation du droit d'accès d'un abonné à ses données

[708] Elle avait non seulement violé l'obligation d'accomplir les formalités préalables à la mise en œuvre de traitements mais aussi l'obligation de mettre à jour les données, le droit d'opposition, l'obligation d'information des personnes concernées, l'obligation de sécurité des données, l'obligation de répondre aux demandes de la CNIL (délibération n° 2008-470 du 27 novembre 2008 de la formation restreinte prononçant une sanction pécuniaire à l'encontre de la société ISOTHERM, disponible sur : http://www.cnil.fr/en-savoir-plus/deliberations/deliberation/delib/204/).

[709] Délibération n° 2008-422 du 6 novembre 2008 portant décision de la formation restreinte à l'égard de la société CDISCOUNT, disponible sur : http://www.cnil.fr/en-savoir-plus/deliberations/deliberation/delib/147/.

[710] Délibération n° 2007-049 du 15 mars 2007 sanctionnant la société STUDIO REPLAY, disponible sur : http://www.cnil.fr/en-savoir-plus/deliberations/deliberation/delib/152/.

nominatives [711]. Quant à la société JSPM qui envoyait des messages publicitaires par télécopie, celle-ci a été condamnée à une amende de 5.000 euros pour manquement à l'obligation de recueillir le consentement préalable des personnes concernées, à l'obligation d'accomplir les formalités préalables à la mise en œuvre des traitements et pour non-respect du droit d'opposition [712]. Par ailleurs, il apparaît que la CNIL condamne plus sévèrement les comportements réalisés en violations du de la loi IFL que le juge pénal. Plusieurs raisons peuvent justifier cette différence. Tout d'abord, la sanction financière choisie par la CNIL ne sera effectivement appliquée que si le contrevenant ignore l'avertissement qui lui est adressé ou ne se conforme pas à la mise en demeure. Cet entêtement de ce dernier peut alors justifier la fermeté de la Commission. En revanche, dans le cadre d'un procès pénal, le responsable du traitement ne bénéficie pas de la possibilité de modifier son comportement, le juge répressif tranchera le litige au regard de l'infraction constatée. Par ailleurs, cette différence peut encore s'expliquer par le fait que pour le juge pénal, les infractions à la loi IFL sont considérées d'un degré de gravité moindre par rapport à la criminalité traditionnelle à laquelle il doit fréquemment se confronter [713].

258. Le cumul des sanctions administratives et pénales. En cas de violation de la loi IFL, les victimes peuvent saisir de façon simultanée l'une des deux juridictions compétentes, à savoir la juridiction pénale ou la CNIL, l'une n'étant pas exclusive de l'autre. Le Conseil Constitutionnel a admis le cumul des sanctions prononcées, sous réserve que le montant global des deux peines ne dépasse pas le montant le plus élevé de l'une des deux sanctions prononcées [714] et ce, afin de ne pas heurter le principe de procédure pénale *non bis in idem* selon lequel nul ne peut être poursuivi ou condamné pénalement à raison des mêmes

[711] Délibération n° 2008-163 du 12 juin 2008 prononçant une sanction pécuniaire à l'encontre de la société NEUF CEGETEL, disponible sur : http://www.cnil.fr/en-savoir-plus/deliberations/deliberation/delib/149/

[712] Délibération n° 2010-232 du 17 juin 2010 de la formation restreinte prononçant une sanction pécuniaire à l'encontre de la société JPSM, disponible sur : http://www.cnil.fr/en-savoir-plus/deliberations/deliberation/delib/248/.

[713] V. en ce sens Fabrice MATTATIA, « CNIL et tribunaux : concurrence ou complémentarité dans la répression des infractions à la loi informatique et libertés », *Rev. sc. crim. et de dr. pénal comparé* avril-juin 2009, p. 316 et s., spéc. p. 328.

[714] Conseil Constitutionnel, décision n° 89-260 du 28 juillet 1989, Loi relative à la sécurité et à la transparence du marché financier : si « *l'article 8 de la Déclaration des droits de l'homme et du citoyen dispose notamment que " la loi ne doit établir que des peines strictement et évidemment nécessaires ",* […] *la possibilité n'en est pas moins reconnue à la Commission des opérations de bourse de prononcer une sanction pécuniaire* […] *susceptible de se cumuler avec des sanctions pénales prononcées à raison des mêmes faits et pouvant elles-mêmes atteindre un montant identique ; que, si l'éventualité d'une double procédure peut ainsi conduire à un cumul de sanctions, le principe de proportionnalité implique, qu'en tout état de cause, le montant global des sanctions éventuellement prononcées ne dépasse pas le montant le plus élevé de l'une des sanctions encourues ; qu'il appartiendra donc aux autorités administratives et judiciaires compétentes de veiller au respect de cette exigence* ». – V. ég. Conseil Constitutionnel, décision n° 97-395 du 30 décembre 1997, Loi de finances pour 1998 : « *lorsqu'une sanction administrative est susceptible de se cumuler avec une sanction pénale, le principe de proportionnalité implique qu'en tout état de cause, le montant global des sanctions éventuellement prononcées ne dépasse pas le montant le plus élevé de l'une des sanctions encourues ; qu'il appartiendra donc aux autorités administratives et judiciaires compétentes de veiller au respect de cette exigence* ».

faits. La loi IFL prévoit ainsi que « [l]*orsque la Commission nationale de l'informatique et des libertés a prononcé une sanction pécuniaire devenue définitive avant que le juge pénal ait statué définitivement sur les mêmes faits ou des faits connexes, celui-ci peut ordonner que la sanction pécuniaire s'impute sur l'amende qu'il prononce* » [715]. Si cette solution permet de renforcer la répression des infractions à la loi IFL et de compenser la faiblesse des peines prononcées par le juge pénal, le montant des sanctions financières prononcées par la CNIL reste encore trop faible pour avoir un effet réellement dissuasif. En définitive, la publicité de la sanction apparaît comme « *la véritable sanction* » [716] en raison de l'atteinte à l'image et à la réputation qui en découlent et peut ainsi avoir des conséquences économiques graves pour le contrevenant.

259. La proposition tendant à renforcer le pouvoir de sanction de la CNIL : une initiative non pertinente. Les auteurs de la proposition de loi de 2009 « *visant à mieux garantir le droit à la vie privée à l'heure du numérique* » suggèrent un renforcement des pouvoirs de sanction de la CNIL [717] en doublant les montants de 150.000 et 300.000 euros actuellement en vigueur. Selon eux, cette revalorisation des sanctions pourrait permettre à la Commission de manifester une plus grande sévérité face aux infractions constatées, à l'instar de son homologue espagnol. En effet, ce dernier a prononcé des sanctions d'un montant total de 22,6 millions d'euros sur la seule année 2008 contre 520.400 euros pour la formation restreinte de la CNIL depuis sa création en 2005 [718]. Cette modification est, selon nous, artificielle dans la mesure où les dispositions venant sanctionnées les comportements en infraction à la loi IFL sont déjà élevés, voire trop élevés pour certains d'entre eux [719] sans pourtant que le *maximum* des *quanta* prévus soient prononcés. Ainsi, est-il permis de douter que le réhaussement des peines incite d'une part, les requérants à davantage agir sur le fondement de ces textes pénaux et d'autre part, les juges à prononcer des sanctions plus sévères. Dans ces circonstances, il est possible de soutenir que l'efficacité de la loi pénale ne dépendra pas d'une modification des textes dans le sens d'une plus grande sévérité mais résultera davantage d'une plus grande cohérence entre la gravité de l'infraction et la sanction à laquelle le contrevenant s'expose.

*****

[715] Art. 47, al. 2 loi n° 2004-801.
[716] Fabrice MATTATIA, « CNIL et tribunaux : concurrence ou complémentarité dans la répression des infractions à la loi informatique et libertés », art. préc., spéc. p. 329.
[717] Art. 12 proposition de loi, 6 nov. 2009, préc.
[718] Art. 12 Proposition de loi préc., spéc. pp. 6-7.
[719] Sur cette critique, v. *supra* : n° 246.

*** * ***

260. Les menaces que fait peser le *spamming* sur les données à caractère personnel imposaient de s'interroger d'une part, sur les garanties offertes par les lois sur la protection des données et d'autre part, sur leur capacité à appréhender les nouvelles formes de *spamming* ou, le cas échéant, à évoluer pour les prendre en compte. S'agissant de cette seconde question, la proposition de loi française de 2009 atteste que notre droit national est perfectible et peut donc s'adapter aux menaces qui apparaissent au rythme du développement des nouvelles technologies. Quant à la première question, il est apparu que nonobstant la détermination ferme du législateur français de construire un régime de protection des données solide, les résultats de sa mise en œuvre sont l'aveu d'un échec, au moins partiel. En effet, face à la violation manifeste par le « spammeur » des principes directeurs en matière de collecte et de traitement des données ainsi que des obligations qui lui incombent, il était fort souhaitable que le volet pénal de loi de 2004 s'impose comme un instrument de répression dissuasif, garant du respect et du fonctionnement du dispositif informatique, fichiers et libertés. Les espoirs de son succès étaient nourris par une multiplication des incriminations et le rehaussement des peines. Toutefois, ces attentes ont été largement déçues au regard de la faiblesse des sanctions prononcées à l'encontre des « spammeurs » dans les rares contentieux dénombrés. De même, malgré le renforcement des pouvoirs de la CNIL et son implication croissante dans l'application de la loi IFL, le montant des sanctions financières prononcées s'avère peu dissuasif et ne permet donc pas de compenser la faiblesse du droit pénal. À l'inverse, il sera observé aux États-Unis que, malgré un système de protection contrasté qui reste à uniformiser, sa mise œuvre est plus rigoureuse.

SECTION II. AUX ÉTATS-UNIS, UNE PROTECTION CONTRASTÉE À UNIFORMISER

261. Une protection sectorielle des bases de données privées. Le système juridique de protection américain se voit souvent reprocher par les Européens son excessive tolérance face au traitement des données à caractère personnel. Cette critique procède notamment d'une approche différente de celle choisie en Europe où cette problématique est considérée comme prioritaire. Pour autant, les questions relatives à la protection des données ne sont ni ignorées du débat législatif, ni absentes du paysage doctrinal et jurisprudentiel [720]. À cet égard, le *Privacy Act*, adopté en 1974 [721], et applicable à l'ensemble de l'administration fédérale, énonce des principes similaires à ceux du droit français en matière de collecte et de traitement des données nominatives gérées par cette dernière et traduisant une préoccupation incontestable du législateur américain pour la protection de ce type de données [722]. Néanmoins, attaché à une logique économique prépondérante, le système américain privilégie une autorégulation minimale et pragmatique en matière de protection des bases de données gérées par le secteur privé, qui limite l'intervention du législateur aux seuls cas où l'autorégulation ne fonctionne pas. Son action législative se manifestera donc ponctuellement à travers une série de lois à portée limitée, destinée à répondre à un problème précis et touchant un type spécifique de données et de gestionnaires de traitement.

262. L'influence européenne. Sous l'impulsion de l'évolution observée dans les législations étrangères et notamment européennes, la question de la protection des données a été progressivement renouvelée aux États-Unis. En particulier, l'essor de la circulation et des échanges transnationaux des données a conduit à l'adoption de la directive européenne 95/46/CE qui impose aux États qui opèrent des échanges internationaux impliquant des

[720] Fondé sur les principes de liberté et de responsabilité, le souci de « *fair information* » (information honnête) inspire la doctrine et la jurisprudence mais aussi le monde de l'entreprise et son organisation. Invoqué dès 1973 par le ministère de la santé (*Health, Education, and Welfare Department)*, ce principe induit quatre mesures à adopter : « *1 – notice : informer les gens des pratiques et des finalités de la collecte et du traitement de données permettant d'identifier des personnes. 2 – access : l'intéressé doit avoir accès aux banques de données qui le concernent, et pouvoir corriger ou éliminer certaines données. 3 – consent and choice : l'intéressé doit pouvoir exprimer son accord ou désaccord sur la collecte et la diffusion, à des tiers notamment, de données personnelles, et sur la durée de leur conservation. 4 – security ; l'information doit être exacte, protégée efficacement contre toute entreprise frauduleuse, le vol, la disparition* » (Pierre TABATONI, « Stratégies de la privacy aux États-Unis. La dynamique des systèmes de protection » *in* Pierre TABATONI (sous la dir.), *La protection de la vie privée dans la société de l'information*, P.U.F., coll. *Cahiers sciences morales*, Paris, 2002, spéc. p. 233).

[721] 5 *U.S.C.* Sec. 552 a. – Rappelons qu'avant cette loi, un comité consultatif créé en 1973 avait publié le premier code des pratiques de l'information loyale (*Code of Fair Information Practices*), code dont les Européens se sont plus tard inspirés pour élaborer leurs lois générales en matière de protection des données.

[722] On retrouve dans le *Privacy* notamment le principe de la transparence, les droits d'accès et de rectification, la limitation de la collecte des données, de leur usage et de leur divulgation, le principe de sécurité et de qualité des données et la responsabilité des gestionnaires de traitement (Pour une étude intéressante de cette loi, v. Suzanne INNES-STUBB et Robert GELLMAN, « L'approche américaine : la régulation par le congrès, le marché et le juge » *in Informatique : servitude ou libertés ?*, colloque préc.).

données nominatives d'origine européenne, de garantir un niveau de protection équivalent à celui existant dans l'Union Européenne [723]. Les influences européennes ont dès lors joué comme un signe avant-coureur d'une évolution croissante vers un système juridique plus protecteur des données. Après une évolution timide si l'on en juge le panorama législatif désordonné existant avant 2005 (§ 1.), celle-ci n'a cessé de se confirmer à partir de 2005, ouvrant ainsi la voie vers une protection plus homogène (§ 2.).

§ 1. AVANT 2005 : UN PANORAMA LÉGISLATIF DÉSORDONNÉ

263. Une protection disparate : délimitation de l'étude. En l'absence de législation générale relative aux données à caractère personnel, le panorama législatif américain se présente comme un *patchwork* de lois, sans grande cohérence les unes avec les autres et dont la portée est limitée au seul domaine pour lequel elles ont été édictées. Ce constat se vérifie dans le secteur privé où le champ de la réglementation des traitements de données est circonscrit à certaines catégories de données et de responsables de fichiers exclusivement visés par la loi considérée [724]. Notre propos n'est pas d'énumérer l'ensemble des lois américaines destinées à protéger les données nominatives [725] mais plutôt, à partir de celles susceptibles de s'appliquer en matière de *spamming*, de comprendre comment le système juridique américain s'évertue à encadrer l'utilisation de ce type de données. Parmi les quatre lois fédérales considérées comme principales aux États-Unis – le *Children's Online Privacy Protection of 1998* [726], le *Gramm-Leach-Bliley Act* (GLBA) [727], le *Fair Credit*

[723] Sur l'exigence de protection adéquate, v. *supra* : n° 219.

[724] Le secteur public assurant une meilleure protection que le secteur privé et notamment une protection plus large avec le *Privacy Act* de 1974 (5 *U.S.C.* Sec. 552a, préc.), loi fédérale destinée à réguler les activités de l'État fédéral et à encadrer les relations avec les pouvoirs publics et les droits des citoyens.

[725] Pour une étude très complète et approfondie de l'approche américaine en matière de protection des données à caractère personnel et des principales lois adoptées en la matière, v. Suzanne INNES-STUBB et Robert GELLMAN, « L'approche américaine : la régulation par le congrès, le marché et le juge » *in Informatique : servitude ou libertés ?*, colloque préc.

[726] Le *Children's Online Privacy Protection Act* (COPPA) (15 *U.S.C.* 6501-6506) qui protège la collecte en ligne de données nominatives des mineurs (sur cette loi, v. *infra :* n° 264).

[727] Adopté par le Congrès le 12 novembre 1999, cette loi relative à la modernisation des services financiers (*The Financial Modernization Act*) (15 *U.S.C.* 6801-6809), connue également sous le nom de « *Financial Services Modernization Act of* 1999 », est entrée en vigueur le 13 novembre 2000. Cette loi a notamment supprimé toutes les barrières existantes entre les banques commerciales, les sociétés de placement et les compagnies d'assurances qui peuvent désormais librement s'affilier. Toutefois, cette évolution n'est pas sans risque puisque les institutions financières disposent désormais d'un accès à une immense quantité de données nominatives sur leurs clients leur permettant de les exploiter, de les analyser et de les vendre. Se rapprochant ainsi progressivement de la logique européenne et de l'esprit de la loi française du 6 août 2004, la loi américaine vise à protéger la confidentialité des données à caractère personnel des consommateurs détenues par les institutions financières et transitant entre ces dernières. À ce titre, la *Federal Trade Commission* a rédigé un guide à l'attention des entreprises pour une meilleure application du GLBA. (v. " How To Comply with the Privacy of Consumer Financial Information Rule of the Gramm-Leach-Bliley Act - A Guide for Small Business from the Federal Trade Commission ", juillet 2002, disponible sur :

Reporting Act [728], le *Health Insurance Portability and Accountability Act* [729] – seule la première d'entre elles sera brièvement examinée. Nous nous attacherons à l'étude du *Children's Online Privacy Protection* dans la mesure où les services de l'internet (forums de discussions, chat, messagerie électronique, sites de réseaux sociaux…) sont utilisés par un public de plus en plus jeune. Cette accessibilité croissante de l'internet laisse ainsi penser que, parmi les données collectées par le « spammeur », certaines d'entre elles peuvent concerner des mineurs de moins de treize ans, auquel cas le *Children's Online Privacy Protection of 1998* aura vocation à s'appliquer.

264. L'exemple de la protection des données des mineurs, une priorité étasunienne. La protection des données à caractère personnel des mineurs de moins de treize ans est considérée aux États-Unis comme un objectif prioritaire de politique publique. Le Congrès a ainsi adopté le 19 octobre 1999 le *Children's Online Privacy Protection Act* (COPPA), entré en vigueur le 21 avril 2000, qui fixe les règles en matière de collecte, d'enregistrement, d'utilisation et de diffusion des données nominatives de mineurs de moins de treize ans collectées en ligne [730]. Cette loi fait suite au rapport établi par la FTC et présenté au Congrès en juin 1998, dans lequel elle réitérait ses préoccupations quant aux dangers de la collecte en ligne de données nominatives auprès de ce jeune public. Contrairement au droit

---

http://www.ftc.gov/bcp/edu/pubs/business/idtheft/bus67.shtm). – Pour des détails sur cette loi, v. not. FTC, " *The Gramm-Leach-Bliley Act - Privacy of Consumer Financial Information* ", disponible sur : http://www.ftc.gov/privacy/glbact/glboutline.htm). – Pour un contexte historique plus détaillé de cette loi, v. par exemple : *Electronic Privacy Information Center* (EPIC), " *The Gramm-Leach-Bliley Act* ", disponible sur : http://epic.org/privacy/glba/.

[728] Le *Fair Credit Reporting Act* (FCRA) (15 *U.S.C.* 1681 et seq.), loi encadrant l'utilisation des données relatives au statut de crédit des consommateurs (disponible sur : http://www.ftc.gov/os/statutes/031224fcra.pdf). Alors qu'en France, cette pratique reste peu courante et cantonnée au crédit à la consommation, le *credit-score* est omniprésent dans tous les actes de la vie quotidienne des consommateurs américains (souscription d'un forfait de téléphonie mobile, signature d'un contrat de bail ou l'obtention d'un crédit immobilier). Développée par les établissements de crédits, cette méthode bancaire (*scoring*) permet, grâce à un programme de traitement de données nominatives, d'évaluer le risque lié à une demande de crédit en fonction d'un score attribué à chaque consommateur et qui détermine la probabilité pour ce dernier d'être éligible à la qualité d'emprunteur. La place prépondérante occupée par le système du *credit-scoring* dans la société américaine a conduit le législateur à créer en 1970 une loi destinée à encadrer spécialement ce domaine, le FCRA. Destinée à protéger les consommateurs américains contre une utilisation abusive de leurs informations relatives aux positions de crédit recueillies par les agences de notation financière (*consumer reporting agencies*), cette loi réglemente les droits d'accès et de rectification des données par le consommateur, similaires au système français, ainsi que les conditions dans lesquelles ces agences sont autorisées à communiquer les fichiers et scores à des tiers.

[729] Le *Health Insurance Portability and Accountability Act* (HIPPA) (42 *U.S.C.* Sec. 201 et seq.) protège les données nominatives touchant le domaine de la santé. Cette loi fédérale a autorisé le ministère de la santé à émettre des règles de protection pour ce type de données qui sont entrées en vigueur en 2003 (45 *C.F.R.* Parts 160 & 164.). La réglementation s'applique aux fournisseurs de service de soins (médecins, pharmaciens, cliniques, organismes d'accréditation) et aux organismes de prévoyance et de compensation (pour des précisons, consulter le site du ministère de la santé, disponible sur : http://www.hhs.gov/ocr/privacy/.)

[730] 15 *U.S.C.* 6501-6506. – Pour des précisions sur cette loi et un détail de l'ensemble des dispositions, consulter : http://www.coppa.org/ et le site de la FTC : http://www.ftc.gov/privacy/coppafaqs.shtm. – Pour une critique de cette loi, v. not. Valérie STEEVES, « La protection en ligne de la vie privée des enfants », *in* 29e Conférence des Commissaires à la protection des données et de la vie privée, 27 septembre 2007, disponible sur : http://www.privacyconference2007.gc.ca/workbooks/Terra_Incognita_workbook10_bil.pdf.

français qui ne dispose pas de texte spécifique en la matière [731], cette loi vise à encadrer strictement la collecte et l'exploitation des données à caractère personnel des mineurs. Elle impose notamment à tout gestionnaire d'un site *Web* commercial à destination des enfants ou leur proposant un service internet [732] d'afficher clairement leur politique en matière de protection des données, en précisant la nature des informations collectées auprès de ces mineurs, l'usage qui en sera fait et si ces dernières sont susceptibles d'être transmises à des tiers [733]. En pratique, la politique adoptée en matière de protection des données doit figurer sur la page d'accueil du site Internet et un lien vers cette politique doit être présent sur toutes les pages *Web* où des informations nominatives de mineurs sont susceptibles d'être collectées [734]. En outre, les coordonnées d'un contact, son adresse électronique ou toute autre information similaire doivent être mentionnées sur le site [735]. Les responsables de sites internet sont également tenus d'obtenir le consentement des parents avant toute collecte, utilisation et divulgation de ces informations [736]. La loi est très stricte en la matière puisqu'elle parle de « *consentement parental vérifiable* », c'est-à-dire que les exploitants de site Internet doivent prendre toute mesure raisonnable pour s'assurer que les parents sont avertis des pratiques du site en matière de collecte, d'utilisation et de divulgation de données auprès des enfants et qu'ils soient en mesure d'y consentir. Par ailleurs, cet accord doit être obtenu avant toute collecte, utilisation et divulgation de ces données [737]. Le responsable du site ou le service en ligne doit également fournir, sur demande des parents, des informations concernant leur(s) enfant(s), une description des types d'informations collectées auprès de ce(s) dernier(s), et leur permettre de refuser toute utilisation ou collecte future par le site de données relatives à leur(s) enfant(s) [738]. Enfin, le responsable du site ou le service en ligne doit mettre en place et maintenir des procédures raisonnables destinées à protéger la confidentialité, la sécurité et l'intégrité des données nominatives collectées [739]. En matière de sanction, la FTC a très sévèrement condamnée les atteintes à la COPPA. À ce titre, elle a par exemple prononcé une amende d'un million de dollars à l'encontre du réseau social XANGA.COM pour la violation des dispositions de cette loi [740], amende à laquelle a également

[731] La CNIL a établi une série de recommandations, v. Cécile ALVERGNAT (Rapport CNIL présenté par), *Internet et la collecte de données personnelles auprès des mineurs*, 12 juin 2001, disponible sur : http://w3.scola.ac-paris.fr/juniors/droits/mineurs.pdf.
[732] 15 *U.S.C.* Sec. 6501 (10) (A).
[733] 15 *U.S.C.* Sec. 6502 (b) (1) (A) (i).
[734] 15 *U.S.C.* Sec. 6501(4).
[735] 15 *U.S.C.* Sec. 6501(12).
[736] 15 *U.S.C.* Sec. 6502 (b) (1) (A) (ii).
[737] 15 *U.S.C.* Sec. 6501 (9).
[738] 15 *U.S.C.* Sec. 6502 (b) (1) (B).
[739] 15 *U.S.C.* Sec. 6502 (b) (1) (D).
[740] *United States of America (for the FTC), Plaintiff, v. Xanga.com, Inc., a corporation, John Hiler, individually and as an officer of the corporation, and Marc Ginsburg, individually and as an officer of the corporation, Defendants (U.S. District Court for the Southern District of New York)*, Civil Action n° 06-CIV-6853(SHS), FTC n° 062-3073, 7 sept. 2006, disponible sur: http://www.ftc.gov/os/caselist/0623073/index.shtm et

été condamnée la société SONY BMG MUSIC ENTERTAINMENT en 2008 mais que cette société avait accepté de régler pour mettre fin aux poursuite engagées contre elle [741]. Force est d'admettre que, malgré l'existence d'un système seulement sectoriel, le montant très élevé des sanctions prononcées démontrent que les juges entendent appliquer rigoureusement les lois existantes. Cette rigueur doit être saluée car elle permet de garantir aux données couvertes par la loi considérée une protection nettement plus efficace que celle assurée par le système français [742].

265. Un système de protection globalement insuffisant. De façon générale, si chaque loi sectorielle peut offrir certaines garanties de protection aux titulaires des données nominatives [743], il n'en demeure pas moins incontestable que la multiplicité des lois fédérales, largement disparates et désunies, tend à affaiblir ces efforts législatifs. En effet, cette situation conduit à ce qu'une même catégorie de données soit réglementée par plusieurs lois offrant un niveau de protection distinct et sans cohérence. Cette fragilité législative tend à s'aggraver en raison du manque d'effectivité dont souffrent les mécanismes de mise en œuvre et de respect de ces lois. Pour l'essentiel, les lois fédérales en matière de protection des données ont tendance à confier à l'administration le respect des lois, en refusant d'accorder un droit d'agir aux personnes physiques [744]. Les institutions américaines chargées de contrôler ou de veiller à l'application de la protection des données ne jouissent pour l'essentiel d'aucun rôle substantiel ni ne dispose d'aucune compétence générale, qu'il

http://www.ftc.gov/opa/2006/09/xanga.shtm.

[741] *United States of America (For the FTC), Plaintiff, v. Sony Bmg Music Entertainment, a general partnership subsidiary of Sony Corporation of America, Defendant (U.S. District Court For the Southern District of New York)*, Case n° 08 CV 10730 (LAK), FTC File n° 082 3071, 11 déc. 2008, disponible sur : http://www.ftc.gov/os/caselist/0823071/index.shtm et http://www.ftc.gov/opa/2008/12/sonymusic.shtm (en l'espèce, la FTC reprochait à SONY BMG MUSIC ENTERTAINMENT la violation de la COPPA pour l'insuffisance d'informations figurant sur ses sites *Web* quant aux données qu'elle collectait en ligne auprès de mineurs, à la façon dont elle les utilisait et à ses pratiques en matière de divulgation de telles données. La FTC lui reprochait d'avoir collecté et divulgué *via* un millier de sites *Web* des données nominatives de centaines de mineurs de moins de treize ans sans le consentement de leurs parents, tel qu'imposé par la COPPA et de ne pas avoir fourni à ces derniers des moyens raisonnables leur permettant de vérifier les informations personnelles sur leurs enfants qui avaient été collectées afin de pouvoir, le cas échéant, s'opposer à toute nouvelle utilisation ou conservation de ces données. La FTC avait ainsi demandé le versement d'un million de dollars d'amende civile, l'interdiction pour cette société de toute violation de la COPPA ainsi que l'effacement de toutes données collectées et maintenues en infraction à cette loi. Il était exigé de la société qu'elle distribue au personnel de sa société cette injonction ainsi que la recommandation de la FTC intitulée " *How to Comply with the Children's Online Privacy Protection Rule* ". Elle enjoignait également à cette société d'insérer un lien vers la section relative à la *privacy* des mineurs sur tous les sites *Web*sur lesquels elle opèrait et qui tombaient dans le champ de la COPPA).

[742] Rappelons à cet égard que le montant maximal des sanctions financières prononcées par la CNIL ne dépasse que très rarement 30.000 euros (sur ce point, v. *supra :* n°257).

[743] Comme il a été précédemment précisé, rappelons que quarante-cinq des cinquante États américains disposent d'une législation contraignante en matière de transparence en cas de menaces à la sécurité des données.

[744] Tel le cas du *Children's Online Privacy Protection Act* dont le respect de ses dispositions est assuré exclusivement par la FTC et les *Attorneys* généraux des États ou encore du *Gramm-Leach-Bliley* dont le respect est assuré par les régulateurs bancaires fédéraux, les autorités de contrôle des assurances des États et la FTC.

s'agisse des administrations fédérales ou du secteur privé [745]. L'espoir d'une protection plus homogène s'est toutefois renforcé à partir de 2005 grâce à plusieurs propositions de loi œuvrant en ce sens.

§ 2. À PARTIR DE 2005 : LES PRÉLUDES Á UNE PROTECTION PLUS HOMOGÈNE

266. Les exigences d'une protection renforcée. Le 24 janvier 2005, en réaction à la recrudescence des vols d'identité sur l'internet et des atteintes à la sécurité des données nominatives [746], les sénateurs démocrates, notamment Patrick LEAHY et Arlen SPECTER ont tenté de souligner l'importance de ces problèmes. Souhaitant mettre en exergue l'inefficacité des lois en vigueur face aux développements des technologies et l'ingéniosité des auteurs des vols d'identité, ils ont présenté successivement plusieurs propositions de loi devant le Congrès américain qui tendent à se rapprocher de l'esprit de la législation européenne. Parmi ces textes, on peut citer le *Privacy Act* [747] et le *Personal Data Privacy and Security Act of 2005* [748]. Tandis que le premier vise notamment à protéger la confidentialité des informations relatives aux internautes en exigeant le consentement d'un individu avant la vente et la

[745] Pour une étude approfondie des failles de ces mécanismes, v. Suzanne INNES-STUBB, Robert GELLMAN, « L'approche américaine : la régulation par le congrès, le marché et le juge », *in Informatique : servitude ou libertés ?*, colloque préc., spéc. p. 102 et s.

[746] US Department of Homeland, *The Crimeware Landscape : Malware, Phishing, Identity Theft and Beyond*, octobre 2006, disponible sur : http://www.antiphishing.org/reports/APWG_CrimewareReport.pdf (ce rapport met en évidence une recrudescence, entre 2005 et 2006, des vols d'informations sensibles *via* des logiciels malveillants qui permettent d'obtenir toute sorte d'informations confidentielles, notamment les noms d'utilisateurs, leurs mots de passe, les numéros de carte bleu, de compte bancaire, de sécurité sociale, et des informations personnelles comme la date d'anniversaire ou le nom de jeune fille de la mère. Ce rapport constate que ces maliciels dédiés au vol d'identité représentent un problème en croissance rapide. Les attaques de *phishing* sont également de plus en plus réalisées grâce à ces logiciels malveillants : entre mai 2005 et mai 2006, leur nombre a presque triplé. Par ailleurs, le rapport observe que le nombre de sites *Web* qui héberge ce type de logiciels connaît une augmentation exponentielle puisqu'en mai 2005, il n'en comptait que 495 pour atteindre en avril 2006, le nombre de 2683). – V. ég. ANTI-PHISHING WORKING GROUP, *Phishing Activity Trends*, août 2006, disponible sur : http://www.antiphishing.org/reports/apwg_report_August_2006.pdf. – De nombreuses sociétés américaines ont subi de graves failles de sécurité et des millions d'américains ont été exposés à des vols d'identité. Parmi elles, on peut citer la société CHOICEPOINT, *leader* du courtage de données nominatives qui, en février 2005, a été victime d'un piratage de informatique entraînant le vol des noms, adresses et numéros de sécurité sociale de 150.000 personnes figurant dans ses bases de données. Le même mois, la *BANK OF AMERICA* a perdu une bande informatique sur laquelle étaient sauvegardées 1,2 millions de données à caractère personnel. Un mois plus tard, l'un des concurents de CHOICEPOINT, la société LEXISNEXIS a déclaré avoir subi le vol de données nominatives de 310.000 individus (pour une liste chronologique des affaires intervenues en matière de vols de données, v. not. Declan MCCULLAGH, " LexisNexis flap draws outcry from Congress ", 12 avril 2005, disponible sur : http://news.cnet.com/LexisNexis-flap-draws-outcry-from-Congress/2100-7348_3-5668119.html?tag=mncol;txt et les différents liens).

[747] S. 116, *Privacy Act*, 109th Congress, Session 1st, présenté le 24 janvier 2005 par le Sénateur démocrate Dianne FEINSTEIN, connue aussi sous le nom de « Identity Theft bill » qui restera également à l'état de projet de loi (pour plus d'informations, voir l'adresse suivante : http://thomas.loc.gov/).

[748] S. 1332, *Personal Data Privacy and Security Act of 2005*, 109th Congress, Session 1st, présenté le 29 juin 2005 janvier 2005, connue aussi sous le nom de « Identity Theft bill » (pour de plus amples informations, consulter l'adresse suivante : http://thomas.loc.gov/). – Guillaume JAHAN, « Personal Privacy and Security Act : combattre le détournement des données personnelles sur Internet », art. préc.

commercialisation de ces données, le second est destiné à combattre les vols d'identité, assurer le respect de la vie privée, alourdir les sanctions pénales, garantir une assistance à l'application de la loi et autres protections contre les atteintes à la sécurité des données, l'accès frauduleux et la mauvaise utilisation d'informations personnellement identifiables. Ces deux propositions de lois de 2005 annoncent une protection future plus large des données (A.). Toutefois, le *Personal Data Privacy and Security Act* de 2005 sera seulement cité ici à titre introductif [749] puisque l'essentiel de ses dispositions sera repris dans une proposition de loi du même nom présentée en 2009 [750] et pour laquelle il sera consacré un développement particulier (B).

A. LES PROPOSITIONS DE LOIS DE 2005 : L'AMORCE D'UNE PROTECTION PLUS LARGE

267. Un champ d'application élargi. Aspirant à rompre avec l'approche législative classique caractérisée par une intervention sectorielle et ponctuelle des lois, le *Privacy Act* de 2005 aurait vocation à réglementer, non seulement les activités des administrations mais encore celles des acteurs privés. Son champ d'application est également élargi au travers des définitions fixées puisque toutes les informations personnelles identifiantes (*personally identifiable information*) sont concernées. Cette catégorie regrouperait les nom, prénom, adresse physique et adresse électronique, numéro de téléphone, photographie ou toute forme d'identification visuelle d'un individu, y compris la date d'anniversaire, le numéro de certificat de naissance ou encore le lieu de naissance, et toutes informations concernant cet individu combiné avec une ou plusieurs des données précédemment énumérées [751]. Par ailleurs, cette proposition organise un régime spécial pour certaines données, comme les identifiants sociaux [752], les données nominatives à caractère financier [753], les données relatives à la santé [754] ou encore les numéros de permis de conduire [755].

[749] Le projet de loi de 2005 n'est jamais devenu une loi, lui a succédé un autre projet de loi du même nom, S. 1789, 109 th Congress, Session 1st, présenté le 29 septembre 2005 par les sénateurs démocrates Arlen SPECTER, Patrick LEAHY, Dianne FEINSTEIN, and Russel FEINGOLD qui a connu le même sort.
[750] S. 1490, *Personal Data Privacy and Security Act of 2009*, 111th Congress, 1st Session, présenté le 22 juillet 2009 et rapporté au *Committee* le 5 novembre suivant, disponible sur : http://www.govtrack.us/congress/bill.xpd?bill=s111-1490.
[751] S. 116, Sec. 104 (7).
[752] S. 116, Sec. 201-210.
[753] S. 116, Sec. 301-306.
[754] S. 116, Sec. 401-407.
[755] S.116, Sec. 501.

268. Un contrôle par les titulaires de données plus accru. Une entité commerciale ne pourrait vendre les données à des tiers, à moins que la personne concernée en soit préalablement informée [756] et que celle-ci soit mise en mesure de limiter leur divulgation et leur cession [757]. Cette initiative tendrait à rendre plus transparentes les manipulations opérées sur les services en ligne et à apaiser le mécontentement des groupes de discussion de consommateurs américains qui considèrent l'usage de leurs données comme abusif. Toutefois, les opérations de collecte et de traitement des données seraient autorisées dès lors qu'elles seraient réalisées par l'entreprise elle-même, notamment à des fins de prospection commerciale [758].

269. Un droit à l'information renforcé. Selon cette proposition de loi, la personne concernée devrait être informée de l'identité de l'entité commerciale rassemblant les données, des types d'informations personnelles collectées, de la manière dont elles seraient utilisées, les catégories de destinataires potentiels ainsi que les modalités d'opposition à l'utilisation ou à la cession de ces données [759]. Cette information devrait intervenir avant la vente ou l'utilisation de ces données de telle façon que la personne concernée puisse disposer d'un délai raisonnable pour évaluer les renseignements qui lui seraient notifiés et fixer les limites de cette vente ou de cette utilisation [760]. S'agissant des modalités de cette information, d'une manière générale, celle-ci devrait être claire et visible [761] et pourrait être transmise par le même moyen que celui qui sera utilisé pour la collecte des données [762]. Par ailleurs, les restrictions énoncées par le titulaire des données concernant la vente de ses données à des tiers non affiliés ou leur divulgation à des fins commerciales seraient réputées permanentes sauf mention contraire [763]. Dans le cas où il accepterait leur vente ou leur divulgation, la révocation de son consentement resterait néanmoins toujours possible et à tout moment. L'entité commerciale serait tenue de mettre en mesure l'individu d'exercer son opposition grâce à des moyens simples et dans la forme utilisée lors de la collecte. Cette liberté ne pourrait toutefois pas jouer lorsque la divulgation des données s'avèrerait nécessaire à la conclusion de la transaction commerciale [764].

[756] S. 116, Sec. 101 (a) (1) (A).
[757] S. 116, Sec. 101 (a) (1) (B).
[758] S. 116, Sec. 101 (a) (2).
[759] S. 116, Sec. 101 (b) (1).
[760] S. 116, Sec. 101 (b) (2).
[761] S. 116, Sec. 101 (b) (4).
[762] S. 116, Sec. 101 (b) (3).
[763] S. 116, Sec. 101 (c) (2).
[764] S. 116, Sec. 101 (c) (4).

270. Dans l'attente d'une évolution plus concrète. Malgré les avancées certaines en matière de protection des données à caractère personnel, le *Privacy Act of 2005* et le *Data Privacy and Security Act* n'ont jamais été soumis au vote du Congrès, se heurtant à de virulentes critiques qui leur reprochaient notamment d'être défavorables au monde des affaires. Toutefois, la seconde proposition n'est pas restée définitivement lettre morte puisqu'en 2007, les vents politiques ayant tourné et le marteau législatif [765] ayant changé de main, les sénateurs LEAHY et SPECTER ont à nouveau présenté une proposition de loi, le *Personal Data Privacy and Security Act* [766] en joignant leurs forces aux Sénateurs démocrates Dianne FEINSTEIN et Russ FEINGOLD [767]. Toutefois, faute encore une fois d'avoir pu être adoptée en tant que loi, lui succèdera le *Personal Data Privacy and Security Act of 2009* [768] qui reprend, en substance, des dispositions très similaires.

B. LES ESPOIRS NOURRIS PAR LE *PERSONAL DATA PRIVACY AND SECURITY ACT OF* 2009

271. Même si cette proposition n'est pas encore adoptée, il est important d'en étudier les principales dispositions en raison de son caractère unique. En effet, dans le cas où elle deviendrait une loi, elle aurait vocation à s'appliquer très largement aux *data brokers* [769], à toutes les entreprises qui rassemblent des informations sensibles personnellement identifiables [770] mais aussi au gouvernement fédéral lui-même. Parmi ses dispositions majeures, figurent des obligations en matière de traitement des données (1.), l'obligation de mettre en place un programme de sécurité des données (2.), ainsi que des dispositions relatives à sa mise en application (3.).

---

[765] Aux élections de mi-mandat du 9 novembre 2006, les démocrates contrôlaient les deux chambres du congrès. Le parti démocrate américain avait remporté la majorité absolue à la Chambre de représentants (la chambre basse), le président de cette chambre (*speaker*), troisième personnage de l'État était Madame Nancy PELOSI.

[766] S. 495, 110th Congress, 1st Session, Report n° 110-70.

[767] Cette proposition se révélait ambitieuse puisqu'elle visait à équilibrer les intérêts et besoins respectifs des consommateurs, des entreprises et du gouvernement fédéral, tout en assurant une meilleure protection des données personnelles des Américains. Ce texte consolidait ainsi les propositions de réforme entamées en 2005 en donnant la priorité à la lutte contre le vol d'identité, les atteintes à la sécurité, la confidentialité des données, l'accès frauduleux et la mauvaise utilisation des informations personnellement identifiables par le biais d'une obligation d'informer de l'existence de failles de sécurité et d'une aggravation des sanctions pénales.

[768] S. 1490, *Personal Data Privacy and Security Act of 2009*, proposition de la loi préc.

[769] Il s'agit d'entités d'affaires (*business entities)* qui pratiquent régulièrement, au sein des États, des opérations de collecte, transmission, ou fournissent un accès à des informations sensibles personnellement identifiables sur plus de 5.000 individus à des tiers non affiliés (S. 1490, Sec. 3 (3)).

[770] Appartiennent à cette catégorie toute information ou compilation d'informations sous une forme électronique ou digitale servant comme moyen d'identification. Il peut s'agir d'un nom ou d'un numéro qui peut être utilisé seul ou combiné avec d'autres informations permettant d'identifier spécifiquement un individu tels que : un nom, un numéro de sécurité sociale, un permis de conduire, un numéro de passeport, une donnée biométrique unique (empreinte digitale, voix, image de la rétine ou de l'iris de l'œil ou autres moyens de représentation unique…) (S. 1490, Sec. 3 (9)).

1. Les obligations en matière de traitement des données

272. Les entités qui maintiennent des données personnelles seraient tenues au respect d'une obligation de transparence strictement encadrée (a.) et d'une obligation de mettre en place un programme de sécurité des données (b.).

a. Une obligation de transparence strictement encadrée

273. Conditions de fond. En cas de découverte d'une atteinte à la sécurité des données (*data security breach*), les entités d'affaires [771] et les agences fédérales [772] devraient en informer, « *dans un délai raisonnable* » [773], les individus concernés ainsi que les personnes chargées d'appliquer la loi [774]. Armés d'une telle connaissance, les consommateurs pourraient ainsi prendre des mesures appropriées pour assurer la protection de leurs données. Cette information serait requise à partir de l'instant où il existerait un risque significatif de dommage (*significant risk of harm*) [775]. Cette condition permettrait ainsi d'empêcher toute notification excessive, ou au contraire insuffisante, tout en assurant une protection efficace des consommateurs. En prenant pour référence le terme de « dommage » plutôt que celui de « vol d'identité », la proposition de loi aurait ainsi vocation à appréhender de façon plus large l'ensemble des préjudices susceptibles de survenir et notamment ceux provenant d'un manquement à l'obligation de sécurité, d'un préjudice physique ou encore de menaces à la sécurité nationale.

274. Exceptions. Il existerait toutefois des exceptions à cette exigence de transparence [776]. Tel serait le cas par exemple lorsque des questions relatives à la sécurité nationale ou à l'application de la loi seraient en cause. En effet, les agences ou les entités d'affaires seraient exemptées de cette obligation dès lors qu'elles certifieraient par écrit au Service secret qu'une telle notification ferait obstacle à une enquête sur l'application de la loi

[771] Ce terme regroupe notamment toute organisation, société, cartel, association, entreprise individuelle, ou entreprise établie pour faire un bénéfice ou à but non lucratif (S.1490, Sec.3 (3)).
[772] Il s'agit de chaque autorité du Gouvernement des États-Unis, à l'exclusion notamment du Congrès, des tribunaux des États-Unis, des gouvernements des territoires ou possessions des États-Unis, du Gouvernement du District de Columbia, des cours martiales et commissions militaires (S.1490, Sec.3 (1) renvoyant au 5 *U.S.C.* Sec. 551).
[773] Est considéré comme un délai raisonnable le temps nécessaire pour déterminer l'étendue de l'atteinte à la sécurité constatée, empêcher toute divulgation future de données, restaurer l'intégrité du système de données et en informer, le cas échéant, les personnes chargées de l'exécution de la loi (S.1490, Sec. 311 (c) (2)).
[774] S. 1490, Sec. 311 (a)
[775] S. 1490, Sec. 312 (b) (1) *a contrario*.
[776] Outre, celle relative à l'absence de risque significatif de préjudice.

ou porterait préjudice à la sécurité nationale, à charge pour le Service secret d'en évaluer les mérites [777]. Serait également exonérée de cette obligation toute entité d'affaire qui disposerait ou utiliserait un programme de sécurité pour prévenir des fraudes financières [778]. De surcroît, afin d'éviter tout risque de notification excessive ou insuffisante, la proposition de loi suggère de fournir aux agences et entités d'affaires l'opportunité d'évaluer pleinement les manquements à l'obligation de sécurité des données. Dans les quarante-cinq jours de la découverte de l'atteinte à la sécurité, les résultats de cette évaluation et leur décision de faire valoir cette exception devraient être adressés au Service secret [779] qui devrait alors apprécier la pertinence de ce choix et se prononcer dans les dix jours suivant la réception de cette décision [780].

275. Conditions de forme. Cette information pourrait être formulée par écrit à la dernière adresse postale connue de l'individu et enregistrée par l'agence ou l'entité d'affaires, par téléphone en contactant personnellement l'individu, ou par courrier électronique si l'individu y a consenti [781]. Quel que soit le média utilisé pour transmettre cette information, cette dernière devrait inclure une description des catégories d'informations sensibles identifiantes qui auraient été ou dont on pourrait raisonnablement croire qu'elles auraient été acquises par une personne non autorisée. Elle devrait également préciser un numéro d'appel gratuit permettant à l'individu de contacter l'agence (ou l'entité d'affaires) dont les bases de données auraient été affectées par cette atteinte afin de connaître quels types de données cette entité détiendrait sur lui [782].

b. L'obligation de mise en place d'un programme de sécurité des données

276. Contenu de l'obligation. Le titre III de la proposition de loi exigerait des entreprises qui rassemblent, ont accès, transmettent, utilisent, stockent ou disposent

[777] S. 1490, Sec. 312 (a).
[778] S. 1490, Sec. 312 (c).
[779] S. 1490, Sec. 312 (b) (2).
[780] S. 1490, Sec. 312 (b) (3).
[781] S. 1490, Sec. 313.
[782] S. 1490, Sec. 314. – Il existe également des notifications spéciales : lorsque la notification a vocation à être adressée à plus de 5.000 individus, les agences et les entités d'affaires doivent signaler cette faille à toutes les agences d'évaluation des consommateurs (*consumer reporting agencies*) qui compilent et conservent des fichiers sur les consommateurs (S. 1490, Sec. 315). Les agences et entités d'affaires doivent également aviser le Service Secret des États-Unis de toute atteinte à la sécurité des données si celle-ci implique plus de 10.000 individus, ou touche une base de données contenant des données concernant plus d'un million d'individus à l'échelle nationale ou une base de données du gouvernement fédéral, ou encore concerne des employés du gouvernement ou des personnes impliquées dans la sécurité nationale ou la mise en application de la loi (S. 1490, Sec. 316 (a)). Dans ces différentes hypothèses, la notification doit intervenir au plus tard, dans les quatorze jours de la survenance de cette faille (S. 1490, Sec. 316 (c)).

d'informations personnellement identifiables concernant plus de 10.000 citoyens américains, la création d'un programme de sécurité des données [783]. Cette obligation ne s'imposerait toutefois pas aux institutions financières déjà soumises aux exigences de sécurité fixées par le GLBA et aux entités régies par le *Health Insurance Portability and Accountability Act* (HIPPA) [784]. À défaut d'appartenir à l'une des deux exceptions précitées, les entités devraient créer un programme de sécurité exhaustif et clair, incluant des mesures de protection administratives, techniques et physiques appropriées à la taille et à la complexité de l'entreprise ainsi qu'à la nature et à l'ampleur de ses activités [785]. Ce programme devrait être conçu pour assurer la sécurité, la confidentialité, l'intégrité des données sensibles personnellement identifiables, les protéger contre toutes sortes d'atteintes possibles et accès non autorisés qui pourraient causer un risque de dommage ou de fraude significatif à tout individu [786]. À cette fin, les entités seraient tenues de procéder à une évaluation minutieuse des risques potentiels qui pourraient résulter d'un accès non autorisé à ces informations [787]. Tout programme devrait être conçu en fonction des risques identifiés afin d'adopter des mesures adéquates au regard du caractère sensible des données, de la taille de l'entreprise ainsi que de la complexité et de l'envergure de ses activités [788]. L'entité devrait prendre des mesures destinées à former ses salariés pour qu'ils respectent le programme de sécurité et permettant d'assurer la surveillance de la mise en œuvre de ce programme [789]. Enfin, il appartiendrait aux entreprises d'effectuer régulièrement un test de vulnérabilité de leur programme de sécurité afin de détecter, empêcher et répondre aux attaques, intrusions et autres atteintes au système [790]. De façon générale, toute entité serait soumise à une évaluation périodique des mesures de sécurité auxquelles elle aurait recours et devrait procéder à leur ajustement en cas de changement significatif relatif à la technologie, le caractère sensible des données, les menaces internes et externes et les éventuelles évolutions au sein de cette entité [791].

2. La reconnaissance d'un droit d'accès et de correction

[783] S. 1490, Sec. 301.
[784] S. 1490, Sec. 301 (c).
[785] S. 1490, Sec. 302 (a) (1).
[786] S. 1490, Sec. 302 (a) (2).
[787] S. 1490, Sec. 302 (a) (3).
[788] S. 1490, Sec. 302 (a) (4).
[789] S. 1490, Sec. 302 (b).
[790] S. 1490, Sec. 302 (c).
[791] S. 1490, Sec. 302 (e). – L'Administration des Services Généraux (*General Services Administration*) est responsable de l'examen du programme de sécurité des données mis en place par le *data broker*. À ce titre, elle doit notamment vérifier si le programme répond de façon adéquate aux menaces de sécurité existantes au regard de l'ampleur des bases de données et systèmes compromis et des efforts fournis par le *data broker* pour atténuer l'impact de ces atteintes (S. 1490, Sec. 401(a)).

277. Contenu. Comme dans le(s) proposition(s) de loi de 2005 [792], les individus disposeraient d'un droit d'accès à toutes les données les concernant qui figuraient dans les bases de données d'un *data brokers* au moment de cette demande et qui seraient destinées à être divulguées à des tiers [793]. À ce droit d'accès, s'ajouterait la possibilité pour toute personne de corriger des informations personnelles détenues par ce *data broker* si celles-ci sont inexactes. Ce dernier serait alors tenu de les mettre en mesure de demander ces rectifications en leur communiquant les instructions sur la procédure à suivre pour obtenir les corrections nécessaires [794]. En cas d'information erronée ou incomplète qui serait conservée dans ses bases de données, le *data broker* serait tenu de vérifier l'exactitude des données contestées et de procéder aux corrections adéquates si elles s'avéraient effectivement incorrectes [795]. Il pourrait toutefois refuser de procéder à cet examen s'il estime, de façon raisonnable, que la contestation de l'individu n'est pas sérieuse ou est motivée par une intention frauduleuse [796]. Dans ce cas, il notifierait sa décision à l'individu dans un temps raisonnable [797].

3. Les sanctions

278. Un volet pénal consolidé. Cette proposition de loi témoigne d'une réelle volonté de mettre fin à cette situation d'insécurité qui pèse sur les données en amendant le Code pénal fédéral pour ajouter à la définition d'activité de racket (*racketeering activity*) l'accès intentionnel et non autorisé à un ordinateur [798]. Toute dissimulation intentionnelle et délibérée d'une atteinte à la sécurité d'informations sensibles personnellement identifiables [799] et qui engendre des dommages économiques à une ou plusieurs personnes, est sanctionnée d'une amende et/ou d'une peine pouvant aller jusqu'à cinq ans de prison [800].

279. Les sanctions civiles. En cas de violation des droits d'accès et de rectification, le *data broker* s'exposerait à des sanctions civiles pouvant aller jusqu'à 1.000 dollars par violation par jour, avec un maximum de 250.000 dollars par violation si le manquement

[792] V. *supra* n° 263.
[793] S. 1490, Sec. 201 (c) (1).
[794] S. 1490, Sec. 201 (c) (2).
[795] S. 1490, Sec. 201 (e).
[796] S. 1490, Sec. 201 (e) (5) (A).
[797] S. 1490, Sec. 201 (e) (5) (B).
[798] S. 1490, Sec. 101.
[799] Parmi les informations sensibles personnellement identifiables, on peut citer : le numéro de sécurité sociale, l'adresse du domicile, la date de naissance, les données biométriques ou encore les informations relatives aux comptes financiers qui seront associés au nom d'un individu.
[800] S. 1490, Sec. 102.

persiste [801]. Tout manquement à l'obligation d'information serait sanctionné d'une amende civile pouvant atteindre 1.000 dollars par jour et par individu dont les données sensibles auraient été collectées ou acquises par des personnes non autorisées avec un maximum de 1.000.000 dollars par violation. Toute violation des exigences légales fixées en matière de sécurité des données serait sanctionnée par une amende civile pouvant atteindre jusqu'à 5.000 dollars par violation et par jour, avec un maximum de 500.000 dollars par violation [802]. Pour l'ensemble de ces incriminations, les peines seraient doublées en cas de violation intentionnelle ou délibérée des obligations fixées [803].

*

* * *

280. Contrairement à certaines idées reçues, si le système juridique américain offre un niveau de protection variable selon les données considérées, cette fragilité est contrebalancée par une effectivité des lois sans conteste bien supérieure. De surcroît, il convient de souligner que le système américain est, à certains égards, plus protecteur que la loi IFL et pourrait se présenter ainsi comme une source d'inspiration intéressante pour faire évoluer notre droit national. Tel est le cas notamment au regard de l'obligation de transparence qui contraint les responsables de traitement à informer les titulaires des atteintes portées à la sécurité de leurs données, obligation que la France devrait intégrer prochainement dans son droit. Enfin, si les initiatives entreprises au cours de l'année 2005 sont le signe d'un progrès à venir en matière de protection des données, celui-ci reste pour le moment à ses balbutiements. En effet, malgré une prise en compte bien réelle des dangers menaçant les données nominatives, associée à un contexte étranger plus protecteur, cette évolution demeure encore à l'état préparatoire, laissant toujours place à un *patchwork* de lois sectorielles. Il ne reste donc qu'à attendre et espérer que cette proposition de loi de 2009, succédant à une série de propositions similaires sans cesse avortées, soit définitivement adoptée auquel cas, ses dispositions n'auraient rien à envier au système de protection français au regard de l'encadrement rigoureux qu'elle assurerait en matière de collecte, d'utilisation et de sécurité des données.

[801] S. 1490, Sec. 202 (a) (1).
[802] S. 1490, Sec. 303 (a) (1).
[803] S. 1490, Sec. 202 (a) (2) ; S. 1490, Sec. 317 (a) ; S. 1490, Sec. 303 (a) (2).

CONCLUSION DU CHAPITRE 1

281. On ne saurait nier que le dispositif de protection français se veut particulièrement protecteur, tant au regard de l'entendue des droits octroyés au titulaire de données que des obligations qui incombent au responsable de traitement mais également des peines prévues en cas de violation de la loi. Toutefois, plus de trente ans après l'adoption de la loi IFL, il est regrettable de constater qu'elle n'a toujours pas eu l'impact attendu. En effet, nonobstant la volonté ferme du législateur français de mettre en place un système de protection fort et ambitieux, la mise en œuvre de la loi IFL dans les cas de *spamming* a révélé que cette dernière souffre d'un « *déficit d'effectivité* », pour reprendre les mots du professeur Jean FRAYSSINET [804]. Nous avons en effet constaté que, malgré l'illicéité manifeste de cette pratique, les poursuites contre les « spammeurs » restent rares et lorsqu'une action est engagée, les sanctions s'avèrent le plus souvent peu dissuasives au regard du faible montant des amendes fixées par les juges. Ce constat met en évidence que ni le volet pénal de la loi IFL ni les sanctions financières prononcées par la CNIL n'apparaissent à la hauteur du niveau de protection annoncé par le législateur. Au-delà des insuffisances de la loi française, la circulation mondiale des données et la dimension internationale du *spamming* imposaient de s'intéresser également aux lois étrangères puisque l'efficacité de la protection des données impose que les législateurs nationaux agissent de concert. Or, les divergences entre les systèmes juridiques françaises et américaines sur cette question sont, pour le moment, manifestes. Il en résulte que chaque fois qu'une situation de *spamming* revêt une coloration internationale, de tels contrastes risquent de compromettre l'efficacité de la protection nationale en vigueur.

[804] Jean FRAYSSINET, « Trente ans après, la Loi "Informatique et Libertés" se cherche encore », chron. préc., spéc. p. 70 et s.

CHAPITRE SECOND : DES LOIS ANTI-*SPAM* PARTIELLEMENT INADAPTÉES AUX SPÉCIFICITÉS DU *SPAMMING*

282. Les défis à relever par les lois anti-*spam*. L'internet s'est révélé être un précieux média de communication pour les annonceurs. Les avantages, tenant notamment au moindre coût des envois et à la possibilité de toucher un public très large, ont multiplié le recours au publipostage électronique. Toutefois, cette évolution a également donné l'opportunité aux « spammeurs » de mener un activité qui parasite le bon fonctionnement des services de messagerie et qui porte atteinte à la tranquillité des internautes. En réaction, les utilisateurs de l'internet sont rapidement devenus de plus en plus méfiants envers les activités qui se développent sur la toile, notamment le commerce électronique. Pour réfréner cette tendance, les législateurs ont dû intervenir [805]. Ils devaient s'attacher à préserver les fonctionnalités des messageries électroniques en permettant aux titulaires de comptes de messagerie de recevoir des *e-mails* d'expéditeurs de confiance et de pouvoir bloquer la réception des messages non désirés.

283. Champ de l'étude. Lors de l'élaboration de leur législation anti-*spam*, les États avaient le choix entre deux régimes distincts pour encadrer les envois, reflet d'une conception dualiste du *spamming* (Section Préliminaire.). Comme nous l'avons souligné au préalable [806], l'effectivité d'une loi dans un contexte international dépend d'une certaine homogénéité entre les systèmes juridiques nationaux. Or, l'analyse comparative des législations anti-*spam* françaises et américaines démontrera que la question de la réglementation des envois commerciaux constitue le point d'achoppement des législations en vigueur de part et d'autre de l'Atlantique : tandis que la première a choisi une prohibition de principe (Section I.), la seconde a opté pour une autorisation de principe (Section II.). Cette analyse nous permettra d'une part d'évaluer l'efficacité de la loi française face aux objectifs de protection fixés et d'autre part, de mesurer plus exactement les différences qui caractérisent chacune des deux lois et les conséquences susceptibles d'en résulter.

[805] Éric BARBRY, « Spam et prospection commerciale : pas de vide juridique mais des modifications nécessaires », *Gaz. Pal.* 22 avr. 2004, n° 113, p. 27 et s. – Laurence MIGUEL-CHESTERKINE, « Quelle protection pour l'internaute contre le publipostage informatique », *LPA* 23 févr. 2000, n° 38, p. 4.
[806] V. *supra* : n° 179..

SECTION PRÉLIMINAIRE. LE CHOIX ENTRE DEUX RÉGLEMENTATIONS DES ENVOIS COMMERCIAUX, REFLET D'UNE CONCEPTION DUALISTE DU *SPAMMING*

284. Définition du problème. La réglementation du *spamming* est traditionnellement envisagée à travers la problématique plus générale de la réglementation des envois commerciaux. Dès l'instant où un État décide d'intervenir pour lutter contre le *spamming*, celui-ci doit définir les moyens de son action, le modèle choisi reflétant la conception qu'il adopte de cette pratique. Concrètement, il existe deux niveaux d'intervention de l'État qui correspondent à deux façons différentes d'appréhender le phénomène de *spamming*. L'une consiste en une intervention « musclée » comme celle existant en Europe où cette pratique est considérée comme une véritable agression de l'internaute. À l'inverse, aux États-Unis, où la protection des intérêts économiques est prioritaire, le législateur a privilégié le développement de la prospection commerciale. Cette alternative rejoint le débat entre l'*opt-in* (§. 1.) et l'*opt-out* (§. 2).

§ 1. L'*OPT-IN* : LA PRIORITÉ CONFÉRÉE À UNE PROTECTION FORTE DES « SPAMMÉS »

285. Portée. Le régime de l'*opt-in* (littéralement, accepter) s'évertue à assurer une prospection conforme à la volonté des destinataires des messages tout en favorisant la création de liens personnalisés entre un professionnel et un internaute prospecté. Dans cette perspective, les envois commerciaux sont donc interdits par principe, à moins que la personne n'ait exprimé son accord. Il en résulte que tout message envoyé sans avoir obtenu le consentement préalable du destinataire est automatiquement considéré comme illicite. Sans interdire dans son ensemble le publipostage commercial par voie électronique, ce principe permet de ne pas légaliser tout type d'envoi qui risquerait d'engorger les boîtes aux lettres des usagers de l'internet.

286. Débat. Si le système de l'*opt-in* se présente comme un système plus protecteur des destinataires, il n'apparaît toutefois pas exempt de certaines critiques. Les détracteurs de ce régime soutiennent que ce choix engendre la paralysie du développement du commerce électronique, l'*e-mail* constituant un outil indispensable pour la prospection commerciale puisqu'il permet de cibler directement les destinataires des messages publicitaires. Il semble en effet que les opérateurs de vente directe apparaissent en pratique

confrontés à de réelles difficultés pour entrer en contact avec des clients potentiels et amorcer une relation permissive dès lors que tout envoi de sollicitations sans le consentement préalable du destinataire leur est interdit. Pour surmonter cet obstacle, certains défendent une conception « pragmatique » de l'*opt-in* qui autoriserait l'envoi d'un premier courrier électronique non sollicité destiné à proposer une inscription en ligne sur un registre d'*opt-in*. Une autre proposition plus restrictive pourrait consister à mettre en place un registre sur lequel les personnes intéressées par un produit ou un service s'inscriraient volontairement, cette inscription matérialisant leur consentement à recevoir des courriers électroniques destinés à promouvoir le produit ou le service choisi [807]. Toutefois, la création de bases de données recensant les internautes qui refusent de recevoir des *e-mails* commerciaux non sollicités constitue un vecteur de risque potentiel pour les données. Facilement accessibles pour les « spammeurs », ces derniers s'empresseront d'exploiter l'ensemble des informations nominatives dont ces listes regorgent. Quelles que soient les modalités pratiques choisies, l'adoption d'une conception trop restrictive de l'*opt-in* conduirait à une situation de blocage dans laquelle les sociétés commerciales se retrouvaient dans l'impossibilité de contacter tout futur client potentiel. À l'inverse, le choix d'un régime trop laxiste donnerait l'opportunité à certains annonceurs malintentionnés de profiter de cette situation et de commettre des abus. Tel pourrait être le cas d'un opérateur qui insère, dans la page introuvable des conditions d'utilisation de son site *Web*, une clause précisant que l'accord préalable donné par l'internaute légitimera le déferlement de futurs messages publicitaires. Le régime de l'*opt-in* nécessite donc que ses bases et limites soient clairement précisées sous peine de devenir inefficace dans la lutte contre le *spamming*.

§ 2. L'*OPT-OUT* : LA PRÉFÉRENCE ACCORDÉE AUX INTÉRÊTS ÉCONOMIQUES

287. Portée. Dans le système de l'*opt-out* (refuser), la pratique du *spamming* n'est pas ressentie comme un comportement agressif et participe au soutien des enjeux et perspectives commerciales. Les envois commerciaux sont donc autorisés par principe. Cependant, toute opposition ultérieure du destinataire manifestant son souhait de ne plus recevoir de nouveaux courriers de la part d'un prospecteur, rendra illégal tout envoi postérieur à cette opposition.

[807] Cette conception serait plus restrictive dans la mesure où l'envoi de messages commerciaux ne porterait que sur des produits ou services que le consommateur connaît déjà.

288. Débat. Parmi les arguments en faveur de l'*opt-out*, ses partisans avancent qu'il est le seul régime permettant d'assurer le développement du commerce électronique. En réponse à cette objection, il convient de souligner que contrairement au régime du consentement préalable, le système de l'*opt-out* ne permet plus au titulaire des données d'en maîtriser leur usage une fois celles-ci collectées [808]. Dès lors, il ne pourra plus être établi de distinction entre le commerçant bienveillant qui envoie des messages à ses clients et le « spammeur » qui aura trouvé une légitimité de façade dans les registres d'opposition. Les difficultés de mise en œuvre apparaissent également lorsque le « spammeur » utilise une adresse électronique usurpée ou inexistante. L'absence d'adresse valide ruinera alors toutes les chances pour le destinataire d'exercer de façon efficace son droit d'opposition. De plus, comme pour les listes d'*opt-in*, leur création risque de donner l'occasion aux « spammeurs » d'accéder à l'ensemble des données à caractère personnel qu'elles contiennent. Outre ce danger, en l'absence de registres centralisés au niveau international, on mesure toute la difficulté que rencontrerait un prospecteur pour vérifier, avant tout nouvel envoi à un destinataire déjà sollicité, si ce dernier ne s'est pas opposé à l'envoi de nouveaux *e-mails* de sa part. Si cette solution était retenue, il devrait alors consulter l'ensemble des registres des États vers lesquels il envisage d'envoyer des courriers électroniques. Cette difficulté s'alourdirait encore dans le cas où l'envoi serait envisagé vers des États qui établissent des registres sectoriels ou vers d'autres qui ne disposent pas de tels registres.

*

* * *

289. L'examen préalable des régimes d'envois commerciaux existants permet de comprendre la logique qui guide chacune de ces deux orientations. En somme, dès lors que le *spamming* est ressenti comme une menace, le législateur optera pour le régime de l'*opt-in*. À l'inverse, si le *spamming* est considéré avec plus de neutralité, c'est-à-dire comme une technique commerciale participant au développement du commerce électronique, le choix du législateur s'orientera vers le système de l'*opt-out.* Cette alternative s'illustre précisément à travers l'opposition entre les systèmes français et américain sur cette question.

[808] Sur la crainte des titulaires de perdre tout contrôle sur leurs données, v. *supra* : n° 165 et s.

SECTION I. EN FRANCE, UNE PROHIBITION DE PRINCIPE

290. L'adoption définitive du régime de l'*opt-in* en France (§. 2.) n'a pas été immédiate et constitue l'aboutissement d'une longue période d'hésitations au cours de laquelle la position des législateurs communautaires s'est illustrée par un mouvement de va-et-vient entre les deux systèmes (§ 1.).

§ 1. L'HÉRITAGE D'UNE ÉVOLUTION COMMUNAUTAIRE HÉSITANTE

291. Entre imprécisions et contradictions. Avant 2002, le cadre communautaire réglementant la prospection commerciale par courrier électronique était principalement composé de trois directives [809]. La directive 97/7/CE du 20 mai 1997, dite « directive vente à distance » [810], opérait une distinction selon le mode d'envoi du message commercial : tandis que le recours à un automate d'appel ou télécopieur entraînait l'application du système de l'*opt-in* [811], les autres moyens de communication à distance, tels que les courriers électroniques ou les SMS, appelaient le régime de l'*opt-out* [812], tout en laissant la possibilité aux États membres de choisir le régime du consentement préalable [813]. Quant aux deux autres directives, la directive 97/66/CE du 15 décembre 1997 [814], dite « Vie privée et télécommunications » [815] et la directive 2000/31/CE du 8 juin 2000 [816], dite « directive sur le

[809] M. Y. SCHAUB, " Unsolicited Email : Does Europe Allow Spam ? The State of the Art of the European Legislation with Regard to Unsolicited Commercial Communications ", 18 *Computer L. & Sec. Rep*. 99 (2002).
[810] Directive 97/7/CE du Parlement européen et du conseil du 20 mai 1997 concernant la protection des consommateurs en matière de contrats à distance, J.O.U.E. n° L. 144 du 4 juin 1997, p. 19 et s.
[811] Art. 10.1 dir. 97/7/CE.
[812] Art. 10.2 dir. 97/7/CE.
[813] Art. 14 dir. 97/7/CE. Usant de cette faculté pour réglementer la pratique du *spamming* sur leur territoire, l'Allemagne, l'Italie, la Finlande, l'Autriche et le Danemark ont ainsi opté pour le régime du consentement préalable.
[814] Directive 97/66/CE du Parlement européen et du Conseil du 15 décembre 1997 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications, J.O.U.E. n° L. 24 du 30 janvier 1998, p. 1 et s.
[815] Cette directive fait application des principes de la directive 95/46/CE (spéc. art.7 dir. 95/46/CE) mais en les adaptant au secteur des télécommunications, la directive 97/66/CE soumet les seules opérations *via* automates d'appels ou télécopieurs au consentement préalable des consommateurs (art. 12-1 dir. 97/66/CE : « *L'utilisation de systèmes automatisés d'appels sans intervention humaine (automates d'appel) ou de télécopieurs (fax) à des fins de prospection directe ne peut être autorisée que si elle vise des abonnés ayant donné leur consentement préalable* »), laissant les États membres libres d'adopter l'un des deux régimes pour les prospections réalisées par d'autres moyens de télécommunication (art. 12-2 dir. 97/66/CE).
[816] Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur, J.O.U.E. n° L. 178 du 17 juillet 2000, p. 1 et s. – Sur cette directive, v. not. Isabelle GAVANON, « La directive " Commerce électronique " : continuité ou nouveauté juridique ?, *Comm. com. électr.* déc. 2001, chron. 28, p. 10 et s. – Luc GRYNBAUM, « La directive " Commerce électronique " ou l'inquiétant retour à l'individualisme juridique », *Comm. com. électr.* juill.-août 2001, chron. 18, p. 9 et s.

commerce électronique » [817], celles-ci se sont gardées de trancher le débat *opt-in* / *opt-out* pour les envois réalisés « *par d'autres moyens de communication* », laissant ainsi les États libres de choisir le dispositif à adopter.

292. Les premières répercussions en France. L'année 2001 a été marquée par de vifs débats qui conduiront à de profondes modifications des dispositions françaises en matière de publipostage électronique [818]. Le 14 juin 2001, le gouvernement français a déposé à l'Assemblée nationale le projet de loi sur la société de l'information [819] qui consacre le régime de l'*opt-out* en matière de publicité non sollicitée par courrier électronique, limitant l'interdiction des envois au seul cas où le destinataire s'est inscrit sur un registre d'opposition [820]. En réaction à ce projet, l'autorité de régulation des télécommunications (A.R.T) a manifesté son désaccord, considérant que ces dispositions ne permettaient pas d'assurer une protection suffisante du consommateur et a encouragé à adopter le régime de l'*opt-in* [821]. Répondant positivement aux vœux de cette autorité, le gouvernement français a rendu public successivement deux ordonnances en 2001 qui transposent partiellement en droit interne les directives 97/66/CE du 15 décembre 1997 [822] et 97/7/CE du 20 mai 1997 [823]. Cette transposition a engendré la création de l'article 33-4-1 du Code des postes et télécommunications (CPCE) et la modification de l'article L. 121-20-5 du Code de la consommation qui transposent l'un et l'autre fidèlement la distinction de régime opérée au niveau européen selon les techniques de communication utilisées en matière de prospection : le consentement préalable des destinataires n'est requis qu'en cas de prospection

[817] Applicable aux seules communications commerciales à distance réalisées exclusivement par voie électronique, la directive 2000/31/CE laisse les États choisir entre l'*opt-in* et l'*opt-out* et se retranche derrière les dispositions des deux directives précitées de 1997 (considérant 30 dir. 2000/31/CE). Ce renvoi aux deux directives de 1997 est confirmé en son article 7.2 qui dispose que : « *sans préjudice de la directive 97/7/CE et de la directive 97/66/CE, les États membres prennent des mesures visant à garantir que les prestataires qui envoient par courrier électronique des communications commerciales non sollicitées consultent régulièrement les registres "opt-out" dans lesquels les personnes physiques qui ne souhaitent pas recevoir ce type de communications commerciales non sollicitées peuvent s'inscrire, et respectent le souhait de ces dernières* »). Le *spamming* est encadré à l'article 7.1 qui impose que les États membres qui autorisent l'envoi d'*e-mails* commerciaux non sollicités, veillent à ce que ces derniers soient clairement identifiés comme tels dès leur réception par le destinataire, sans autre exigence (*opt-out*).

[818] Ariane MOLE et Hélène LEBON, « Publipostage électronique : entre certitudes et incertitudes », 2e partie, *Gaz. Pal.* 13 juill. 2002, n° 194, p. 27 et s.

[819] Laurent FABIUS (présenté par), Projet de loi sur la société de l'information, 14 juin 2001, Doc. A.N. no 3143, disponible sur : http://www.assemblee-nationale.fr/11/projets/pl3143.asp.

[820] Art. 22 du projet de loi préc.

[821] A.R.T, Avis no 2001-423 du 2 mai 2001 sur le projet de loi sur la société de l'information.

[822] Ordonnance n° 2001-670 du 25 juillet 2001 portant adaptation au droit communautaire du Code de la propriété intellectuelle et du Code des postes et télécommunications, J.O. n° 173 du 28 juillet 2001, p. 12132 et s.

[823] Ordonnance n° 2001-741 du 23 août 2001 portant transposition des directives communautaires et adaptation au droit communautaire en matière de droit de la consommation, J.O. n° 196 du 25 août 2001, p. 13645 et s.

commerciale réalisée au moyen d'automates d'appel ou de télécopieur [824], les autres moyens de communication (*e-mails* et SMS) étant régis par le système de l'*opt-out* [825].

293. La consécration définitive de l'*opt-in*. Après avoir adopté une attitude hésitante, le droit communautaire s'est finalement détaché de son approche économique consumériste pour céder la place à un système privilégiant la protection des consommateurs. Cette nouvelle orientation lui permettait ainsi de se rapprocher de la logique adoptée par la loi IFL. En effet, compte tenu de la persistance du *spamming* sur le territoire européen, le législateur devait admettre que cette profusion de textes contradictoires emportait deux effets. D'une part, elle ne pouvait raisonnablement aboutir à assurer un niveau de protection élevé des « spammés » et d'autre part, elle troublait la cohérence des règles relatives à la protection des données à caractère personnel qui consacrait, pour leur part, clairement le principe du consentement préalable à toute collecte de données [826]. C'est dans ce contexte juridique et face au mécontentement grandissant des acteurs de l'internet que la directive 2002/58/CE [827], a été adoptée. Visant à adapter au secteur des télécommunications le régime général de protection des données fixé par la directive 95/46/CE, cette directive se prononce clairement en faveur du principe de l'*opt-in* qui devient applicable à tous les services de communication électroniques : « *l'utilisation de systèmes automatisés d'appel sans intervention humaine (automate d'appel), de télécopieurs ou de courrier électronique à des fins de prospection directe ne peut être autorisée que si elle vise des abonnés ayant donné leur consentement préalable* » [828]. Sur ce modèle, la loi française a ainsi consacré le régime de l'*opt-in* [829], qui révolutionne le monde du *marketing* et de la relation client, « *les*

[824] « *la prospection directe au moyen d'un automate d'appel ou télécopieurs, d'un abonné ou d'un utilisateur d'un réseau de télécommunications qui n'a pas exprimé son consentement préalable à recevoir de tels appels* » (art. 33-4-1 CPCE). – Dans une rédaction similaire, l'article L. 121-20-5, al. 1er du Code de la consommation dispose : « *est interdite la prospection par un professionnel, au moyen d'automates d'appel ou de télécopieurs, d'un consommateur qui n'a pas exprimé son consentement à recevoir de tels appels* ». Malgré cette similitude, l'article 33-4-1 CPCE a un champ d'application plus large puisqu'il n'est pas limité aux seuls prospecteurs « professionnels ».

[825] Art. 121-20-5, al. 2 C. conso.

[826] En ce sens, v. Vincent VARET, « Le cadre juridique du *spam* : état des lieux », *Comm. com. électr*. sept. 2002, chron. 21, p. 14 et s., spéc. p. 16.

[827] Dir. préc.

[828] Considérant 40 et article 13.1 dir. 2002/58/CE. – En Europe, la plupart des États ont choisi le système l'*opt-in*, notamment l'Allemagne, la Belgique, l'Autriche, la Finlande, le Danemark ou encore l'Italie (v. Ariane MOLE et Hélène LEBON, « Publipostage électronique : entre certitudes et incertitudes », 1re partie, *Gaz. Pal*. 18 avr. 2002, n° 108, p. 29 et s.).

[829] Sur le projet de loi relatif à la confiance dans l'économie numérique, v. par ex. Thomas DAUTIEU, « Le nouveau régime juridique applicable à la prospection directe opérée par voie électronique (À propos du projet de loi relatif à la confiance dans l'économie numérique) », *Gaz. Pal*. 1er nov. 2003, n° 305, p. 8 et s. – Étienne DROUARD, « À propos de la loi " économie numérique " et débat " *opt-in* "/" *opt-out* ", il n'est pas encore interdit de réfléchir », Expertises 2004, n° 277, pp. 16-17. – Luc GRYNBAUM, « Loi " Confiance dans l'économie numérique " : une version définitive proche de la version originale de la Directive " commerce électronique " », *Comm. com. électr*. juin 2004, comm. 78, p. 38 et s., spéc. p. 40.

entreprises ayant eu, jusqu'alors, l'habitude de considérer qu'elles avaient le droit de s'adresser en particulier à qui elles le souhaitaient et non pas à qui le désirait » [830].

§ 2. LE RÉGIME DE L'*OPT-IN*

294. La loi pour la confiance dans l'économie numérique du 21 juin 2004 (ci-après la LCEN) [831], considérée comme la « *loi destinée au marché* » [832], a pour objectif de regagner la confiance des internautes, ces derniers étant considérés comme moins bien armés et informés pour se prémunir contre les risques liés au commerce électronique [833]. L'œuvre législative s'annonçait dès lors à la fois ambitieuse et délicate puisqu'il s'agissait de fixer les conditions de régularité des envois tout en parvenant à élaborer une subtile conciliation entre des intérêts, par nature, contradictoires : ceux des internautes qui aspiraient à leur tranquillité et à la sécurité de leurs données [834] et ceux des annonceurs attachés à l'exploitation commerciale des nouveaux supports électroniques. Soucieuse d'aboutir à cet équilibre, en adoptant le régime de l'*opt-in*, la LCEN a pu être saluée comme un véritable texte de compromis [835]. Entérinant le travail ébauché par la CNIL, cette solution permet ainsi d'établir

[830] Jean-Marc COBLENCE, « Le statut de la publicité dans la LCEN », *Comm. com. électr.* sept. 2004, Étude 25, p. 28 et s., spéc. n° 12 (ce professionnel du droit, avocat à la cour, estime que « [l]*a prospection publicitaire, formidable prélude à l'acte de commerce, se trouve ainsi entravée par une loi censée promouvoir le commerce électronique* » (*id., loc. cit.*). Il considère le régime de l'*opt-in* comme « *une contrainte exceptionnellement forte au développement du commerce électronique, sans que l'on sache si* […] *elle est rendue nécessaire pour des motifs techniques de sécurité ou de volume de trafic sur la toile ou par un véritable souci de protéger la vie privée des consommateurs et interdire le commerce des adresses et bases de données* » (*id.*, spéc. n° 11).

[831] Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, J.O. n° 143du 22 juin 2004, p. 1168 et s. – Pour une analyse des dispositions relatives aux courriers électroniques non sollicités, v. not. Éric A. CAPRIOLI et Pascal AGOSTI, « La confiance dans l'économie numérique (Commentaires de certains aspects de la loi pour la confiance dans l'économie numérique) », *LPA* 3 juin 2005, n° 110, p. 4 et s. – Nicolas MATHEY, « Le commerce électronique dans la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique », *Cont. conc. conso.* oct. 2004, Étude 13, p. 7 et s. – Sur l'aspect pénal de la loi et son influence sur le Code de procédure pénale et le Code pénal, v. not. Agathe LEPAGE, « LCEN. Libertés sur Internet. Cybercriminalité », *Comm. com. électr*. sept. 2004, Étude 24, p. 24 ; *Dr. pénal* déc. 2004, n° 12, Étude 24, p. 24 et s.

[832] Xavier LINANT DE BELLEFONDS, « De la LCI à la LCEN », *Comm. com. électr.* sept. 2004, Étude 22, p. 9 et s., spéc. n° 1.

[833] Dans cette perspective, ses rédacteurs ont voulu se « *concentrer sur les aspects purement économiques du nouvel ordre informatique, c'est-à-dire essentiellement le commerce électronique* » en se focalisant sur la relation « *B2C et non B2B : la confiance dont on recherche le renforcement est évidemment celle du consommateur et non celle du professionnel que l'on suppose dûment armé pour affronter les risques du commerce à distance* » (Xavier LINANT DE BELLEFONDS, « De la LCI à la LCEN », art. préc., *loc. cit.*). – Jean-Michel BRUGUIERE remarque également une « *instrumentalisation du droit au profit* […] *d'intérêts économiques* » (« " Deux ou trois choses… " que nous savons de la LCEN », *Cont. conc. conso.* déc. 2004, Étude 19, spéc. n° 4). – V. ég. Olivier CACHARD, « Définition du commerce électronique et loi applicable », *Comm. com. électr.* sept. 2004, Étude 31, p. 53 et s. – Jean-Marc COBLENCE, « Le statut de la publicité dans la LCEN », étude. préc.

[834] V. *supra* n° 165 et n° 172 et s.

[835] Jean-Michel BRUGUIERE, « La protection du cyber-consommateur dans la loi pour la confiance dans l'économie numérique », art. préc., spéc. p. 62 (« *L'option de la LCEN est une option de compromis* »).

une cohérence avec la loi IFL [836]. Le régime du consentement préalable, devenu désormais le principe en matière d'envois de courriers électroniques commerciaux (A.), est toutefois assorti de certaines exceptions permettant d'offrir une réponse mesurée et ce, afin de ne pas bannir les activités de prospection directe dans leur ensemble (B.).

A. LE PRINCIPE DU CONSENTEMENT PREALABLE

295. Fondements. L'article 22 de la LCEN fixe un régime strict d'interdiction en insérant respectivement aux I et II de cette disposition l'article L. 33-4-1 du CPCE modifié [837], désormais transféré sous l'article L. 34-5 du même Code [838] et l'article L. 121-20-5 modifié du Code de la consommation qui renvoie à ce dernier [839]. L'article L. 33-4-1 du CPCE énonce ainsi qu'« [e]*st interdite la prospection directe au moyen d'un automate d'appel, d'un télécopieur ou d'un courrier électronique utilisant, sous quelque forme que ce soit, les coordonnées d'une personne physique qui n'a pas exprimé son consentement préalable à recevoir des prospections directes par ce moyen* » [840]. En visant également la prospection directe par courrier électronique, les envois commerciaux sont désormais réglementés par un régime unifié quelle que soit la technique de communication à distance utilisée (automates d'appel, télécopieurs, *e-mails*, SMS…) [841]. Il convient à présent d'étudier

[836] En effet, ce choix serait revenu à légitimer la pratique du *spamming* alors même que dès 1999, la CNIL exprimait ses craintes à l'égard de cette pratique et de sa conformité avec la législation existante : « *La pratique du publipostage électronique soulève* […] *des questions qui excèdent le seul champ du commerce électronique et mettent en cause, de manière générale, les règles de protection des données personnelles, notamment les dispositions de la directive 95/46 du 24 octobre 1995 et, en France, de la loi du 6 janvier 1978* » (*Le publipostage électronique et la protection des données personnelles*, rapport préc., spéc. p. 2). Devant l'ampleur de cette pratique, elle fut amenée à dénoncer au Parquet en 2002, certaines entreprises qui se livraient au *spamming* (v. *supra* : n° 190 et s.).

[837] Le Code des postes et télécommunications est devenu le Code des postes et communications électroniques par la loi n° 2004-669 du 9 juillet 2004 relative aux communications électroniques et aux services de communication audiovisuelle, J.O. n° 159 du 10 juillet 2004, p. 12483 et s.

[838] Ce transfert a été opéré par l'article 10-I de la loi n° 2004-669 du 9 juillet 2004, préc. Ses conditions d'application ont été fixées par deux décrets du 27 mai 2005 : le décret n° 2005-605 qui modifie la deuxième partie du CPCE (J.O. n° 124 du 29 mai 2005, p. 9496) et le décret n° 2005-606 relatif aux annuaires et aux services de renseignements et modifiant le CPCE (J.O. n° 124 du 29 mai 2005, p. 9497).

[839] « *sont applicables les dispositions de l'article L.34-5 du Code des postes et télécommunications* » (art. L. 121-20-5 C. conso., al. 1er).

[840] Art. L. 34-5 du CPCE, al. 1er et article L. 121-20-5, al. 2 C. conso.

[841] En l'absence de régime transitoire prévu par la directive 2002/58/CE permettant de régir le sort des fichiers légalement constitués avant la nouvelle loi, lorsque l'*opt-out* était la règle et utilisés postérieurement à l'entrée en vigueur de la nouvelle loi, la France a prévu une disposition particulière. Pour les fichiers valablement constitués avant la promulgation de la LCEN, c'est-à-dire dans le respect des dispositions de la loi IFL, l'article 22 III de la LCEN prévoit que ce type de fichier constitué légalement sous l'empire de la loi de 1978 peut être utilisé pendant une période de six mois mais pour la seule obtention du consentement de l'internaute à recevoir de futurs messages. Cette initiative législative s'inscrit dans un souci d'équilibre auquel est attaché le législateur qui souhaite ne pas sacrifier les intérêts économiques et permettre ainsi aux professionnels de conserver le bénéfice de la valeur des bases de données constituées légalement avant la LCEN.

le champ d'application de cette loi qui, nous le verrons, apparaît trop restrictif à certains égards (1.) avant de s'attacher à la mise en œuvre du régime de l'*opt-in* (2.).

1. Un champ d'application trop restrictif à certains égards

296. En adoptant une position claire en faveur de *l'opt-in*, les articles L. 34-5 CPCE et L. 121-20-5 du Code de la consommation issus de la LCEN marquent une avancée significative par rapport à leur ancienne version qui limitait l'exigence du consentement préalable aux seules prospections commerciales au moyen d'automate d'appel ou de télécopieurs. Désormais, tout envoi de courrier électronique au sens de la loi (a.) à une personne physique (b.) à des fins exclusivement commerciales (c.) est soumis à l'accord préalable du destinataire.

a. La notion légale de courrier électronique

297. Une acception très large opportune. Sur le modèle de l'article 2 (h) de la directive 2002/58/ CE, l'article 1er de la LCEN définit le courrier électronique comme « *tout message, sous forme de texte, de voix, de son ou d'image, envoyé par un réseau public de communication, stocké sur un serveur du réseau ou dans l'équipement terminal du destinataire jusqu'à ce que ce dernier le récupère* » [842]. La loi adopte donc une définition extensive qui permet d'englober tout message transmis par voie électronique et ce, quelle que soit leur nature, à savoir les courriers électroniques classiques, les SMS, les MMS, les systèmes de messagerie vocale, y compris les services mobiles [843]. En choisissant d'adopter une approche technologiquement neutre, le législateur permet ainsi d'adapter le droit aux évolutions technologiques des services de télécommunications, position que la CNIL a, à juste titre, saluée [844]. Cette acception très large de la notion de courrier électronique nous

[842] Art. 1, IV, al. 5 loi n° 2004-575. – Art. 3.1 dir. 2002/58/CE.
[843] CNIL, Guide « *La pub si je veux* », 2008, spéc. p. 9, disponible sur : http://www.cnil.fr/fileadmin/documents/Guides_pratiques/CNIL_Guide_pub.pdf (la CNIL incluant clairement dans la notion de « courrier électronique » les *e-mails*, les SMS et MMS). – V. ég. considérant 67 dir. 2009/136/CE : « *Les garanties apportées aux abonnés contre les atteintes à leur vie privée par des communications non sollicitées à des fins de prospection directe au moyen du courrier électronique devraient aussi s'appliquer aux SMS, MMS et autres applications de nature semblable* ».
[844] Sur ce point, v. « Les observations de la CNIL sur l'article 22 de la loi du 21 juin 2004 pour la confiance dans l'économie numérique », disponible sur : http://www.cnil.fr/es/dossiers/commerce-publicite-spam/halte-au-spam/letat-du-droit-en-france/les-observations-de-la-cnil-sur-larticle-22-de-la-loi-du-21-juin-2004-pour-la-confiance-dans-leconomie-numerique/. – Le Groupe « article 29 » avait précisé, à propos de la directive 2002/58/CE, que l'adoption d'une « *définition vaste et volontairement neutre sur le plan technologique* » visait à inclure les technologies à venir. Il avait ainsi indiqué que la liste énoncée « *ne peut être considérée comme*

semble également circonstanciée puisqu'elle a ainsi vocation à régir les nouvelles formes de *spamming* comme le *spam* par SMS ou le *spam* vocal [845] ou encore les *Blue spams.* À cet égard, la CNIL, lors de sa séance plénière du 11 septembre 2008, a admis sans difficulté que les messages transmis *via* le protocole de communication *Bluetooth* sont considérés comme des courriers électroniques au sens de la loi [846].

298. Une acception large insuffisante : la question des *Blue spams.* Bien que les *Blue spams* soient qualifiés de courrier électronique, il convient néanmoins de souligner que le champ d'application de la LCEN est circonscrit aux seuls messages envoyés « *par un réseau public de communication* » [847], ce qui exclut notamment le réseau *Bluetooth* qui est, par définition, un réseau de communication personnel sans fil [848]. Afin de surmonter cette difficulté, on pouvait espérer que le législateur européen saisisse l'occasion de l'adoption de la directive 2009/136/CE [849] pour étendre le champ d'application de la directive de 2002 afin de prendre en compte les évolutions technologiques, en particulier l'émergence de ces nouveaux modes de communication, tel qu'il l'avait été préconisé à plusieurs reprises lors du réexamen de cette dernière [850]. Contre toute attente, la nouvelle directive de 2009 a maintenu le champ d'application fixé par la directive de 2002 en le limitant aux seuls « *services de*

exhaustive et peut devoir être révisée en considération des développements technologiques et des marchés » (avis n° 5/2004 portant sur les communications de prospection directe non sollicitées selon l'article 13 de la directive 2002/58/CE, 11601/FR, WP 90, 27 février 2004, spéc. p. 4, disponible sur : http://www.cnpd.public.lu/fr/publications/groupe-art29/wp090_fr.pdf).

[845] Sur ces nouvelles formes de *spams*, v. *supra :* n° 99 et s.

[846] CNIL, « Pas de publicité via *Bluetooth* sans consentement préalable », 13 nov. 2008, art. préc.

[847] Art. 1, IV, al. 5 loi n° 2004-575. – Art. 3.1 dir. 2002/58/CE.

[848] Encore appelé réseau individuel de communication sans fil ou réseau domestique sans fil (*Wireless Personal Area Network* (WPAN)).

[849] Directive 2009/136/CE du Parlement européen et du Conseil du 25 novembre 2009 modifiant notamment la directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques, dir. préc.

[850] V. not. G29, Avis n° 2/2008 sur la révision de la directive 2002/58/CE, avis préc., spéc. p. 5 (soulignant la nécessité de prendre en compte « *le développement des réseaux hybrides public/privé* »). – V. ég. Avis du contrôleur européen de la protection des données sur la proposition de directive du Parlement européen et du Conseil modifiant, entre autres, la directive 2002/58/CE, avis préc., spéc. n° 21 et s., p. 5. – Malcolm HARBOUR (présenté par), Rapport au nom de la Commission du marché intérieur et de la protection des consommateurs du 18 juillet 2008 sur la proposition de directive du Parlement européen et du Conseil modifiant notamment la directive 2002/58/CE (2007/0248(COD)), A6-0318/2008, spéc. pp. 91-92, disponible sur : http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+CRE+20080902+ITEM-010+DOC+XML+V0//FR). – Deuxième avis du contrôleur européen de la protection des données relatif au réexamen de la directive 2002/58/CE, avis préc., spéc. n^{os} 62-70, p. 36 et n° 98, pp. 40-41 (proposant d'élargir le champ de la directive de 2002 à tout « *traitement des données à caractère personnel dans le cadre de la fourniture de services de télécommunications électroniques accessibles au public sur les réseaux de communications publics ou sur les réseaux privés accessibles au public dans la Communauté* », excluant ainsi les réseaux privés (*id.* spéc. n° 66, p. 36) et d'insérer la définition suivante *:* « *par réseau privé accessible au public, on entend un réseau exploité de manière privée auquel le public en général a, d'ordinaire, un accès illimité, que ce soit moyennant paiement ou conjointement avec d'autres services ou offres, sous réserve d'acceptation des conditions applicables* » (*Id*, spéc. n° 69, p. 36)). – V. ég. CA Paris, 4 févr. 2005, 14^{e} ch., *BNP Paribas c/World Press Online*, RG n° 04/55398, disponible sur : http://www.foruminternet.org/telechargement/documents/ca-par20050204.pdf (qualifiant de FAI un établissement bancaire qui fournit une connexion à l'internet à son personnel).

communications électroniques accessibles au public sur les réseaux de communication publics » [851]. Il serait donc pertinent que la LCEN, lors de la transposition de la directive de 2009 [852], aille plus loin que cette dernière et englobe les réseaux privés accessibles au public au regard d'une part, de leur multiplication – universités, hôtels, cybercafés, entreprises – et d'autre part, en raison des risques similaires encourus par les données quel que soit le type de réseau considéré [853].

b. Les destinataires, personnes physiques

299. Une protection limitée aux seules coordonnées de personnes physiques. L'alinéa 1er de l'article 22 de la LCEN vise l'utilisation des « *coordonnées d'une personne physique* », excluant ainsi les personnes morales de son champ d'application. À l'occasion de la séance plénière du 1er juillet 2003, la CNIL a précisé une distinction de régime selon que la prospection s'adressait à des adresses impersonnelles du type : contact@societe.fr ou à des adresses électroniques professionnelles sous la forme : nom.prenom@societe.fr. Les premières, étant « *manifestement les coordonnées de personnes morales, le principe du consentement préalable ne s'applique pas, pas plus que les dispositions de la loi du 6 janvier 1978* » [854]. Il en résulte que ce type d'adresses peut continuer à faire l'objet de très nombreuses sollicitations commerciales. En revanche, pour les secondes, le régime d'*opt-in* s'applique pleinement « *dans la mesure où ces adresses permettent l'identification de personnes physiques. L'utilisation à des fins privées ou professionnelles de cette adresse importe peu* » [855]. Cette indifférence quant à la finalité de l'utilisation des adresses se justifie par le fait que les adresses utilisées à des fins professionnelles comportent le plus souvent le nom, voire le prénom d'une personne physique identifiée au sein de l'entreprise destinataire (le responsable des achats, le chef du service de facturation, etc.) et permettent ainsi de désigner sans ambiguïté un individu. Cette indifférence a toutefois suscité de fortes critiques,

[851] Art. 2.3 dir. 2009/136/CE modifiant l'article 3 de la directive 2002/58/CE.
[852] Sur la transposition de la directive 2009/136/CE en droit national, v. Projet de loi portant diverses dispositions d'adaptation de la législation au droit de l'Union européennes en matière de santé, de travail et de communications électroniques, Étude d'impact, Doc. A.N. n° 225, enregistré le 14 septembre 2010, spéc. p. 101 et s., disponible sur : http://www.senat.fr/leg/pjl10-225.pdf.
[853] V. en ce sens, Avis du contrôleur européen de la protection des données sur la proposition de directive du Parlement européen et du Conseil modifiant, entre autres, la directive 2002/58/CE, avis préc., spéc. n° 22, p. 5 (« *La capacité de ces réseaux semi-publics (ou semi-privés) d'empiéter sur la vie privée des personnes est évidente et justifie donc que ce type de services soit soumis aux mêmes règles que les réseaux exclusivement publics* »). – Deuxième avis du contrôleur européen de la protection des données relatif au réexamen de la directive 2002/58/CE, avis préc., spéc. n° 64, pp. 35-36.
[854] CNIL, *Rapport d'activité 2003*, rapport préc., spéc. pp. 65-66.
[855] CNIL, rapport préc., *loc. cit.* ; « Les observations de la CNIL sur l'article 22 de la loi du 21 juin 2004 pour la confiance dans l'économie numérique », préc.

notamment de la part de la Fédération des Entreprises de Ventes à Distance (FEVAD) et du Syndicat National de la Communication Directe (SNCD) qui y voyaient un moyen de paralyser le développement du *marketing* direct, et a conduit la Commission à reconsidérer par la suite sa position [856].

c. Des messages à finalité exclusivement commerciale

300. La prospection directe, seule réglementée par la LCEN. S'il convient de remarquer que l'expression « prospection directe » a quelque chose de tautologique en ce sens que la prospection consiste en une action de rechercher activement de nouveaux clients potentiels afin de les transformer en clients réels. Il semble dès lors difficilement concevable d'envisager une prospection indirecte. « *Toutefois, cette formule permet de distinguer la pratique incriminée*, [c'est-à-dire tournée directement vers telle ou telle personne] *de celle qui s'adresse au public collectivement, comme il en va, par exemple, d'une publicité sur un site* » [857]. Innovant par rapport à la directive de 2002 qui ne se prononçait pas sur la notion de prospection directe, l'article 22 alinéa 3 de la LCEN la définit comme « *l'envoi de tout message destiné à promouvoir, directement ou indirectement, des biens, des services ou l'image d'une personne vendant des biens ou fournissant des services* ». La loi française définit donc cette activité en considération de sa finalité : sont ainsi visés les seuls messages à finalité commerciale [858] ainsi que « *toute forme de promotion de vente* » [859] et ce, quel que soit le mode de communication utilisé. Cette condition nous conduit à réitérer notre souhait de voir entrer les *Blue spams* dans le champ de la LCEN puisque certains d'entre eux peuvent avoir une finalité commerciale. À titre d'illustration, l'enseigne de parfumerie MARIONNAUD a utilisé cette méthode de prospection *via Bluetooth* pour la campagne publicitaire de ses produits [860]. En revanche, tout message qui poursuivrait un but non commercial, à savoir « *le*

[856] Sur l'adoption d'une position nouvelle par la CNIL, v. *infra* : n° 315.
[857] Guillaume TEISSONIERE., « *La lutte contre le spamming : de la confiance en l'économie numérique à la méfiance envers ses acteurs* », *Bull. Lamy*, avr. 2004, n° 168, p. 1 et s., spéc. p. 5.
[858] De même, la loi anti-*spam* américaine limite son champ d'application aux messages à caractère commercia.
[859] G29, Avis n° 5/2004, avis préc., spéc. p. 7 (l'article 13.1 de la directive 2002/58/CE englobe « *toute forme de promotion des ventes, y compris la prospection directe réalisée par les associations caritatives et les organisations politiques (par ex. collecte de fonds, etc.)* ».
[860] En 2007, l'enseigne de parfumerie MARIONNAUD avait envoyé à l'occasion de la fête des mères et des pères des messages publicitaires *via Bluetooth*, invitant les passants à entrer dans ses magasins pour participer à un jeu concours (« Marionnaud au parfum *Bluetooth* », 31 mai 2007, disponible sur : http://www.strategies.fr/actualites/marques/r44927W/marionnaud-au-parfum-bluetooth.html).

démarchage politique, associatif, religieux ou caritatif » est exclu du champ de la LCEN, sans toutefois échapper au respect de la législation relative à la protection des données [861].

301. Un champ d'application inadapté à une lutte globale contre le *spamming*. Cette distinction de régime fondée sur la finalité du message laisse toutefois craindre que, pour tenter d'échapper au respect des obligations fixées par la LCEN, certains annonceurs malveillants plaident le caractère ambigu du contenu des messages envoyés pour contester leur nature commerciale, et soutenir par exemple leur finalité purement informationnelle [862]. Surtout, une telle distinction est difficile à justifier au regard des atteintes que provoque le *spamming*, à savoir l'atteinte à la tranquillité des destinataires, le dysfonctionnement des services de messagerie ou encore la saturation du réseau. En effet, l'ensemble de ces désagréments reste indifférent à la finalité des envois. Pour s'en convaincre, prenons l'exemple des *e-mails* à finalité politique. Si l'indulgence à l'égard de ce type de prospection s'explique en général par un souci de préserver la liberté d'expression des candidats lors des campagnes électorales, nul ne contestera qu'il puisse constituer une véritable nuisance pour les internautes, sollicités chaque jour par un déferlement de messages pendant les périodes électorales [863]. D'une simple nuisance, l'envoi massif de ce type de messages peut même aboutir à une saturation des messageries électroniques. Tel a été le sort par la boîte électronique du Syndicat National des Enseignants du Second degré (SNES) suite de l'envoi d'*e-mails* initié par « La droite libre » qui avait appelé au blocage des boîtes électroniques de ce syndicat [864].

---

[861] Sur ce point, v. « Les observations de la CNIL sur l'article 22 de la loi pour la confiance dans l'économie numérique, relatif à la prospection commerciale par courrier électronique », préc.

[862] À cet égard, il est intéressant de noter que le champ d'application de la loi n° 2004-801 du 6 août 2004 relative à la protection des données à caractère personnel est beaucoup plus large puisqu'il prend en compte tous types de démarches quelle que soit leur finalité. En effet, l'article 38, alinéa 2 prévoit que toute personne physique « *a le droit de s'opposer, sans frais, à ce que les données la concernant soient utilisées à des fins de prospection, notamment commerciale, par le responsable actuel du traitement ou celui d'un traitement ultérieur* ».

[863] La CNIL, sensible aux critiques de certains destinataires, avait souhaité l'application du principe du consentement préalable à figurer dans les fichiers électroniques du parti ou des candidats, fichiers d'adresses qui seraient par la suite utilisés à des fins d'envoi de messages lors des campagnes électorales (délibération n° 2006-228 du 5 octobre 2006 portant recommandation relative à la mise en œuvre par les partis ou groupements à caractère politique, élus ou candidats à des fonctions électives de fichiers dans le cadre de leurs activités politiques, disponible sur : http://www.cnil.fr/en-savoir-plus/deliberations/deliberation/delib/114)/). – V. ég. sur ce point, Jean DIONIS DU SEJOUR et Corinne ERHEL (présenté par), *Rapport d'information sur la mise en application de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique*, Doc A.N. n° 627, 23 janvier 2008, spéc. p. 47 et s., disponible sur : http://www.assemblee-nationale.fr/13/pdf/rap-info/i0627.pdf.

[864] TGI Paris, réf., 26 mai 2003, *SNES* c/ *La Droite Libre et al.*, RG n° 03/54806 , *Juris-Data* n° 2003-211976 ; *Comm. com. électr*. juill.-août 2003, comm. n° 78, p. 40 et s., note A. Lepage. (« La Droite Libre » avait été condamnée au versement de dommages et intérêts pour avoir contraint le SNES à mettre en place des logiciels destinés à stopper ces envois massifs. Pour justifier sa décision, le magistrat avait déclaré que « La Droite Libre » ne pouvait « *se prévaloir d'un exercice normal de la liberté d'expression* […]. *La Droite libre* [a privé]

302. L'opportunité d'élargir le champ d'application. Au regard des perturbations tout aussi importantes que peut causer l'envoi massif *d'e-mails* de nature non commerciale, il semblerait pertinent d'unifier les régimes juridiques applicables aux envois abusifs de messages non sollicités. Cette solution aurait pour mérite d'adopter une juste mesure entre la défense de la liberté d'expression et l'immunité excessive accordée au corps politique susceptible de nuire au droit à être laissé tranquille des internautes [865]. Elle permettrait également de préserver le bon fonctionnement du système d'*e-mail*. Ce souhait est d'autant plus justifié que les courriers électroniques à but non commercial peuvent traiter « *d'un autre sujet dans ces mêmes e-mails* » [866]. Il est tout à fait possible d'imaginer qu'un groupe religieux propose en ligne la vente d'un ouvrage biblique ou encore qu'un parti politique offre la possibilité d'acheter en ligne un ouvrage retraçant la vie du président en fonction. Dans ces différentes hypothèses, le message revêt alors un caractère commercial faisant ainsi douter de la pertinence d'une telle distinction [867]. L'un des objectifs majeurs de la loi française étant de renforcer la confiance des internautes, l'encadrement juridique de toutes les prospections quelle que soit leur finalité – commerciale ou non – permettrait ainsi de limiter encore davantage les risques d'abus. C'est également en ce sens que Jean DIONIS DU SEJOUR, l'un des rapporteurs des travaux élaborés pour la mise en œuvre de la LCEN, s'est prononcé en préconisant l'élargissement de la définition du *spamming* à « *l'ensemble des activités de prospection automatique non désirée, y compris politique et associative* » [868].

2. Les conditions de régularité des envois commerciaux

303. Toute prospection directe est subordonnée à l'exigence de transparence des envois (a.) et au respect du droit d'opposition des destinataires, droit qui a été renforcé avec l'adoption de la LCEN (b.).

---

les demandeurs de l'usage des services de courrier électronique dont [les syndicats] *ont une possession légitime* »).

[865] Sur le droit à être laissé tranquille, v. *supra* : n° 172 et s.

[866] Comme l'a souligné Bruno RASLE (Frédéric AOUN, Bruno RASLE, *Halte au spam*, éd. Eyrolles, 2003.

[867] Cette restriction est d'autant plus difficile à saisir qu'elle apparaît en décalage avec les dispositions de la loi française de 1978 et avec celles de loi de 2004 qui prennent en compte tous types de démarches quelle que soit leur nature (v. art. 38 al. 2 loi n° 2004-801). – On retrouve cette même incompréhension aux États-Unis, v. not. Seth GROSSMAN, " Keeping Unwanted Donkeys and Elephants Out of Your Inbox : The Case for Regulating Political Spam ", 19 *Berkeley Tech. L.J.* 1533, spéc. pp. 1574-1575 (2004) (également favorable à une unification des régimes encadrant les *spams* à caractère commercial et politique dans la mesure où le développement de ces deux types de *spam* s'explique pour les mêmes raisons (coût des envois, facilité de distribution des messages, le nombre très important de destinataires potentiels) et provoque les mêmes dommages. Selon cet auteur, la différence de régime n'est pas justifiée et constitue même « *une sérieuse erreur* » (" *Whatever the reason, the decision to not regulate political spam as part of general regulation of all unsolicited bulk e-mail constitutes a serious mistake* " (*id.*, spéc. p. 1575)).

[868] *Rapport d'information sur la mise en application de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique*, rapport préc., spéc. p. 47.

a. L'exigence de transparence des envois

304. Destinée à garantir une large protection des destinataires, la loi exige des prospecteurs qu'ils expédient leurs messages en toute transparence. Pour cela, ils sont tenus de recueillir le consentement préalable des destinataires en observant strictement les qualités que celui-ci doit revêtir (i.). En pratique, le consentement pourra être recueilli selon diverses modalités (ii.).

i. Les qualités du consentement préalable

305. Sur le modèle de la directive 2002/58/ CE [869], l'article 22 de la LCEN définit le consentement préalable comme « toute manifestation de volonté libre, spécifique et informée par laquelle une personne accepte que des données à caractère personnel la concernant soient utilisées à fin de prospection directe » [870]. Dans un souci de protection des destinataires, la loi exige donc que le consentement recueilli auprès de ces derniers réunisse cumulativement quatre qualités qui seront à mettre en parallèle avec les obligations incombant à tout responsable de traitement de données en vertu de la loi IFL [871].

306. Le principe du consentement « éclairé » et « informé ». La loi impose qu'au moment où la personne donne son consentement, celle-ci soit parfaitement consciente de la portée de son accord. La qualité du consentement dépendra donc de la clarté de l'information préalablement fournie. En pratique, l'information doit préciser sans ambiguïté la finalité commerciale de la collecte et le sort réservé à ces données. En particulier, dans le cas où il est envisagé leur cession ou leur transmission à des tiers à des fins commerciales, une case à cocher autorisant ces opérations doit figurer à côté de celle prévue pour le consentement.

307. Le principe du consentement « libre ». Cette condition prohibe tout obstacle qui tendrait à entraver la liberté de choix du destinataire. Elle assure notamment que le consentement donné est toujours révocable, soit par l'exercice du droit d'opposition au

[869] Art. 2 f) renvoyant à la dir. 95/46/CE, art. 2 h) qui définit le consentement préalable comme « *toute manifestation de volonté, libre, spécifique et informée par laquelle la personne concernée accepte que des données à caractère personnel la concernant fasse l'objet d'un traitement* ».
[870] Art. 34-5 CPCE al. 2 et art. L. 121-20-5 al. 3 C. conso.
[871] Notamment l'article 32 loi n° 2004-801 relatif à l'obligation d'information à laquelle les responsables de traitement doivent se conformer à l'occasion de la collecte de données nominatives (sur cette obligation, v. *infra* : n° 216 et s.).

traitement ultérieur des données, soit en vertu du droit de suppression des données traitées [872]. En aucun cas, le consentement ne doit être accordé sous la pression du prestataire qui refuserait l'envoi de futurs courriers électroniques publicitaires relatifs à d'autres de ses produits ou services à la personne ayant exprimé son opposition.

308. Le principe du consentement « spécifique ». Par « spécifique », il convient de comprendre que le consentement doit émaner de la personne directement et personnellement concernée par le message transmis et être recueilli dès la première prospection et pour chaque nouvelle sollicitation. L'accord donné ne vaut qu'à l'égard du prestataire clairement identifié, pour certains produits et pour une finalité expressément déterminée.

ii. Les modalités de recueil du consentement

309. La « case à cocher » : une solution de compromis. Afin de respecter l'exigence de transparence des envois, il semble qu'une manifestation de volonté trop imprécise ne pourrait être considérée comme répondant aux exigences légales. La CNIL avait précisé à ce titre que la définition du consentement « *exclut que l'expression de ce consentement soit, par exemple, diluée dans une acceptation des conditions générales d'utilisation d'un service proposé ou encore couplée à une demande de bons de réduction* » [873]. Elle avait ainsi recommandé que le consentement soit recueilli « *par le biais d'une case à cocher* » [874], estimant que l'apposition d'une case pré-cochée était « *contraire* […] *au principe de loyauté de la collecte des informations* » [875]. Cette solution protectrice des personnes sollicitées permet ainsi de s'assurer que ces dernières aient donné un consentement « *libre, spécifique et informée* », ce que ne garantit pas la technique de la case pré-cochée. En effet, en retenant le procédé de la case à cocher, il semble difficile de concevoir qu'un prospecteur soit tenté de le faire aux lieu et place de la personne concernée. En revanche, la technique de la case pré-cochée comporte le risque qu'un internaute peu attentif omette par inadvertance de la décocher alors même qu'il ne souhaite pas recevoir de

[872] Sur les droits d'opposition et de suppression des données, v. *supra* n° 224 et s. et 230.
[873] CNIL, délibération n° 02-093 du 28 novembre 2002 portant avis sur le projet de loi relatif à l'économie numérique *in* CNIL, *Rapport d'activité 2002*, rapport préc., spéc. p. 74 et p. 180.
[874] Délibération n° 02-093 préc., *loc. cit.* – En ce sens, v. considérant 17 dir. 2002/58/CE : « *Le consentement peut être donné selon toute modalité appropriée permettant à l'utilisateur d'indiquer ses souhaits librement, de manière spécifique et informée, y compris en cochant une case lorsqu'il visite un site Internet* ».
[875] CNIL, *Rapport d'activité 2002*, rapport préc., spéc. p. 74.

messages publicitaires [876]. Par ailleurs, le G29 a précisé que la technique du « *double opt-in* » qui consiste pour l'internaute à renvoyer à l'expéditeur du message un *e-mail* confirmant son consentement, peut également être utilisée [877]. Toutefois, si cette technique est en pratique garante d'une plus grande sécurité juridique, elle se heurte néanmoins à de réelles difficultés de mise en œuvre. En effet, le recueil du consentement peut se révéler dans certains cas difficile pour les prospecteurs, leur imposer une seconde fois cette obligation pourrait alors devenir une source de complications inextricables et être ressenti comme un moyen de paralyser le développement de l'industrie du *marketing*. Aussi, la mise en place d'un système de « case à cocher » permet d'aboutir à une solution de compromis entre le tout permis (*opt-out*) et son inverse qu'incarne le double *opt-in*.

310. Quelle place accorder au premier *e-mail* de sollicitation? La possibilité de recourir à « *d'autres modalités* » pour recueillir le consentement conduit à s'interroger sur la licéité de la méthode qui consisterait à autoriser l'envoi d'un *e-mail* dont l'objectif serait d'établir un premier contact avec le consommateur, et donc serait, par définition, non sollicité. Deux interprétations de l'article 22 de la LCEN pourraient ainsi être soutenues. Selon une interprétation restrictive de cette disposition, tout message dont la finalité se limite à entrer en relation avec un futur client n'aurait pas vocation à promouvoir « *directement ou indirectement, des biens, des services ou l'image d'une personne vendant des biens ou fournissant des services* ». Préalablement au lancement d'un nouveau produit sur le marché, de nombreuses entreprises mènent des études relatives à son impact et à ses perspectives de succès au regard des attentes des consommateurs. L'internet se révèle alors être un précieux support publicitaire puisque la transmission d'un premier *e-mail* est destiné à inviter les destinataires à se connecter sur le site *Web* où se trouve l'étude proprement dite. À ce stade, il paraît *a priori* possible de considérer que ce premier message n'a pas une finalité commerciale puisqu'il vise seulement à recueillir le consentement de la personne à recevoir des prospections commerciales futures. En effet, ce n'est qu'en cas de succès du sondage réalisé que les futurs messages auront pour finalité la promotion du produit ou du service nouvellement mis sur le marché. À l'inverse, une acception plus large de l'article 22, conduirait à considérer que tout *e-mail* directement envoyé par la personne proposant les biens ou les services participerait à la promotion de son image – cette personne devant s'identifier – et serait dès lors considéré comme une prospection directe. La coexistence de

[876] Avis n° 5/2004, avis préc., spéc. p. 5

[877] *Id., loc. cit.* (selon l'avis n° 5/2004, « *les modalités par lesquelles un abonné donne son consentement préalable en s'enregistrant sur un site Internet et à qui l'on demande par la suite de confirmer son consentement semblent compatibles avec la directive* [2002/46/CE] », tout en précisant que « *d'autres modalités peuvent également être compatibles avec les dispositions légales* »).

ces deux interprétations divergentes est source d'insécurité juridique puisqu'elle risque de voir émerger de multiples décisions d'espèce dont la solution dépendrait de la forme rédactionnelle du message. Le choix entre ces deux interprétations dépend des intérêts que le législateur entend préserver en priorité. Dans un objectif de protection optimal des destinataires, l'interprétation stricte des textes serait privilégiée. Force est d'admettre qu'en pratique, cette solution risque néanmoins de paralyser fortement le développement du *marketing* direct et ôte tout l'intérêt d'utiliser l'internet comme media de prospection pour toucher un très large public. Afin de garantir la tranquillité des internautes sans toutefois sacrifier les intérêts économiques, il semble que la solution la plus raisonnable consisterait en définitive à autoriser les entreprises à envoyer un seul et unique *e-mail* de sollicitation à des clients potentiels [878].

311. Le cas des *Blue spams.* Ces nouvelles techniques de *marketing* de proximité suscitent questionnement quant à leur capacité intrusive et au respect du droit à la tranquillité de l'utilisateur d'un téléphone mobile [879], jugées comme « *particulièrement intrusi*[ves] » par la CNIL [880]. Dans le cas où les *Blue spams* entreraient dans le champ de la LCEN, l'envoi de ce type message serait subordonné au consentement préalable de la personne concernée. La question se pose alors de savoir quelles sont les modalités à respecter pour recueillir le consentement des destinataires. La CNIL a été conduite à se prononcer sur ce point dans une décision du 11 septembre 2008. Selon cette dernière, afin que seules les personnes intéressées par le contenu publicitaire en soient destinataires, ces dernières doivent approcher leur téléphone de quelques centimètres de l'affiche. Le consentement n'est donc valablement recueilli que si c'est le détenteur du téléphone mobile qui manifeste son accord à être prospecté. À cet égard, la CNIL précise clairement que l'envoi systématique de messages publicitaires à toute personne se trouvant dans la zone de couverture d'une affiche ne doit

[878] Clairement opposé à cette alternative, le G29 tranche clairement ce débat en adoptant une interprétation large du texte : « *la simple demande de consentement pour recevoir des courriers électroniques commerciaux par un courrier électronique général envoyé aux destinataires ne serait pas compatible avec l'article 13 de la directive 2002/58/CE* [et pus précisément] *l'exigence selon laquelle la finalité doit être légitime, explicite, et spécifique*°» (Avis n° 5/2004, avis préc., *loc. cit.*).

[879] En réaction à ce nouveau mode de promotion publicitaire, des députés français ont également mis l'accent sur la nécessité de « *déterminer dans quelles conditions la transmission du message* [*via* la technologie *Bluetooth*] *est valide* » (v. en ce sens, *Rapport d'information sur la mise en application de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique*, rapport préc., spéc. p. 46).

[880] CNIL, « Pas de publicité via *Bluetooth* sans consentement préalable », art. préc. – Ce risque d'atteinte à la tranquillité est également susceptible de se poser au regard des nouvelles formes de *marketing* interactif (v. par ex. la technologie *Eye Light* développée par la société française HILABS (www.hilabs.net/fr) qui permet de détecter dans un rayon de 5 m les passants et de leur proposer un message les invitant à feuilleter une annonce publicitaire en faisant glisser leur doigt sur l'écran de la vitrine d'une agence immobilière ou d'une boutique (Patrick CAPELLI, « Les nouveaux explorateurs du continent numérique », 4 févr. 2010, disponible sur : http://www.strategies.fr/actualites/marques/131963W/les-nouveaux-explorateurs-du-continent-numerique.html).

pas constituer le principe [881]. Cette solution mérite approbation dans la mesure où elle permet de protéger les personnes contre la réception incessante de messages publicitaires. Toutefois, dans ce souci perpétuel de protection des personnes prospectées, elle a également ajouté que « *l'envoi d'un message à l'utilisateur s'il accepte l'établissement d'une connexion Bluetooth n'est pas une modalité satisfaisante du recueil du consentement* » dans la mesure où celle-ci interviendrait trop tardivement [882]. Or, comme nous avons eu l'occasion de l'expliquer précédemment, l'activation du mode *Bluetooth* sur son téléphone mobile permet de détecter automatiquement les terminaux qui ont également activé cette fonction. La confirmation du code d'accès permettant l'appairage de deux téléphones mobiles vaut acceptation de l'utilisation de ses données. Afin d'assouplir la position de la CNIL, il a été proposé d'intégrer un « *profil " publicitaire " permettant de distinguer l'usage privé de l'usage commercial et de créer non pas un numéro de série de manière permanente à un terminal mais un numéro Bluetooth dynamique, à l'instar de l'adresse IP* » [883]. Cette proposition permettrait ainsi d'assurer d'une part, une plus grande transparence en informant clairement de la finalité commerciale du message dès la demande d'appairage entre deux terminaux et d'autre part, d'éviter les risques de traçabilité.

b. Le droit d'opposition renforcé

312. Modalités. Afin d'assurer l'effectivité du droit d'opposition des destinataires, l'alinéa 5 de l'article L. 34-5 du CPCE impose non seulement que le prospecteur soit clairement identifié dans le message expédié mais aussi qu'il mentionne une adresse valide à laquelle le destinataire pourra s'adresser pour exercer ce droit. Cette faculté d'opposition doit lui être offerte à l'occasion de chaque nouvel envoi *d'e-mail* commercial. Cette obligation de communiquer les coordonnées du prospecteur prohibe ainsi la dissimulation ou l'usurpation d'identité de l'émetteur de cette communication [884]. Cet impératif soulève toutefois certaines difficultés pratiques en cas d'envoi d'un SMS publicitaire par exemple. En effet, dans ce cas de figure, le nombre limité de caractères rend difficile le respect de cette exigence pour les

[881] CNIL, « Pas de publicité via Bluetooth sans consentement préalable », art. préc. – V. ég. courrier d'Alex TURK, Président de la CNIL, adressé à Christian CHABREBRIE, PDG de la société MOBINEAR, 23 oct. 2008, préc. (« *l'utilisateur doit d'une part, activer Bluetooth sur son mobile et d'autre part, approcher son mobile à moins de 10 centimètres, soit " très près " du détecteur Bluetooth* »).

[882] La CNIL précise qu' « *il est nécessaire de recueillir le consentement préalable du détenteur du téléphone dans la mesure où l'envoi de messages publicitaires sur des téléphones mobiles via la technologie "Bluetooth" constitue une prospection directe au moyen d'un courrier électronique* » disponible sur : http://www.cnil.fr/la-cnil/actu-cnil/article/article/pas-de-publicite-via-bluetooth-sans-consentement-prealable/?tx_ttnews[backPid]=91&cHash=6821270457).

[883] Claire LEVALLOIS-BARTH et Christian LICOPPE, « Le *Bluespam* et la CNIL », *Expertises* 2009, p. 217 et s. , spéc. p. 223.

[884] Art. L. 34-5 CPCE, al. 5 et art. L.120-5-1, al. 6 C. conso., reprenant en substance l'article 13.4 dir. 2002/58/CE.

prospecteurs « *sauf à supprimer l'objet même de leur message, à savoir leur offre promotionnelle ou publicitaire* ! » [885]. Dans ces circonstances, il est fort probable que les annonceurs soient peu enclins à utiliser les nouvelles techniques de communication au profit des plus traditionnelles.

313. Une mise en œuvre compromise en cas de *spamming*. Tel que signalé précédemment, il est rare que le « spammeur » communique une adresse valide destinée à permettre au destinataire du message d'exercer son droit de refuser la réception de nouvelles publicités. Et, quand bien même ce dernier fournirait cette information, celle-ci est la plupart du temps usurpée ou sans cesse renouvelée afin d'échapper à toute traçabilité. Dans ces circonstances, la demande sollicitant l'interruption de tout envoi futur de messages permettrait seulement au « spammeur » de confirmer la validité de l'adresse électronique du destinataire [886].

B. LES EXCEPTIONS AU PRINCIPE DE L'*OPT-IN*

314. Soucieux de garantir les intérêts des sociétés de *marketing* direct, le législateur français a prévu deux exceptions aux principes régissant les envois commerciaux. Ces dérogations correspondent à deux hypothèses : en cas de relations commerciales préexistantes (1.) et lorsque l'adresse électronique destinataire est de nature professionnelle (2.).

1. L'hypothèse des relations commerciales préexistantes

315. Sur le modèle de la directive 2002/58/CE [887], le législateur français, souhaitant faire de la LCEN un véritable texte de compromis, a prévu une exception lorsque l'émetteur d'un message et son destinataire ont été liés par le passé lors de relations commerciales. Dans cette hypothèse, afin de ne pas condamner tous les messages commerciaux non sollicités, la LCEN reconnaît aux sociétés la possibilité de poursuivre, sous certaines conditions, une relation commerciale avec leurs clients, ce qui permet ainsi de parvenir à une

[885] Christophe WILHELM et Annaïck PENVEN, « La prospection commerciale par courrier électronique : le nouvel article L.121-20-5 du Code de la consommation », *Légipresse* oct. 2004, n° 215.
[886] V. *supra :* n° 94.
[887] Art. 13.2 dir. 2002/58/CE.

conciliation, pourtant délicate, entre la prohibition pure et simple du *spamming* et la liberté de communication commerciale.

316. Conditions. Pour que cette tolérance soit accordée, l'alinéa 4 de l'article L. 34-5 CPCE impose le respect de plusieurs conditions cumulatives [888]. Tout d'abord, les coordonnées du destinataire doivent avoir été recueillies directement auprès de ce dernier à l'occasion d'une vente ou d'une prestation de services précédente dans le respect de la loi IFL. Le texte ajoute que la nouvelle prospection directe doit concerner des produits ou services « analogues » à ceux fournis au cours d'une prospection directe précédente et par la même personne physique ou morale. Enfin, elle doit indiquer « *de manière expresse et dénuée d'ambiguïté, la possibilité de s'opposer, sans frais, hormis ceux liés à la transmission du refus, et de manière simple, à l'utilisation de ses coordonnées lorsque celles-ci sont recueillies et chaque fois qu'un courrier électronique de prospection lui est adressé* ». Ces conditions appellent deux séries d'observation : l'une concernant le terme « analogue », l'autre relative à l'exigence d'identité de personne physique ou morale.

317. L'imprécision du terme « analogue ». Il est permis de regretter le manque de précision du terme « analogue ». En effet, comme l'a justement souligné la CNIL, cette situation est une « *source de contentieux* » [889] et une « *source d'interprétations qui ne manqueront pas d'être divergentes* » [890], chaque entreprise risquant de vouloir imposer sa propre conception. Pour tenter de saisir le sens de ce terme, il est possible de se tourner vers la définition fournie par le dictionnaire : est analogue, « *ce qui présente une analogie* » [891], cette dernière notion étant elle-même définie comme « *une ressemblance établie par l'imagination entre deux ou plusieurs objets de pensée essentiellement différents* » [892]. Il apparaît de toute évidence que ces définitions ne sont d'aucun recours. De façon pragmatique, la Commission a mis en évidence les difficultés d'interprétation que soulève cette notion : « *À titre d'exemple, l'opération qui consiste à acheter en ligne un livre autorise-t-elle le vendeur à prospecter l'acheteur pour un disque (un disque est-il un bien analogue à un livre ?) ou pour un voyage (acheter un voyage est-ce un service analogue à l'opération d'acheter un livre en ligne ?)* » [893]. Face à une telle situation, non seulement la sécurité juridique risque d'être compromise mais la protection des données risque également

[888] Art. L. 121-20-5, al. 5 C. conso.
[889] CNIL, délibération 02-093 du 28 novembre 2002, *in Rapport d'activité 2002*, rapport préc., spéc. p. 182.
[890] CNIL, « Les observations de la CNIL sur l'article 22 de la loi pour la confiance dans l'économie numérique, relatif à la prospection commerciale par courrier électronique », préc.
[891] Petit Robert de la langue française, 2001, v. « analogue ».
[892] *Id.* v. « analogie »
[893] Délibération n° 02-093 du 28 novembre 2002, préc., *loc. cit*.

d'être menacée [894]. Afin de clarifier cette notion, le G29 s'était prononcé en faveur d'une interprétation stricte de cette notion en suggérant que celle-ci puisse « *être jugée du point de vue objectif du destinataire (attentes raisonnables), plutôt que du point de vue de l'expéditeur* » [895], solution qui a le mérite de garantir une meilleure protection des destinataires tout en préservant le développement de la publicité en ligne. Il serait judicieux que le législateur français s'inspire, par exemple, de son homologue belge qui, par arrêté royal du 4 mai 2003, s'était attaché à préciser les contours de cette notion en s'appuyant d'exemples concrets et précis. Son article 1er alinéa 5 précise que : « *sont considérés comme produits ou services analogues, ceux qui appartiennent à une même catégorie de produits ou de service. Par exemple – et pour l'heure, à titre conjectural, on pourrait considérer comme analogues les CDs et DVDs, les cassettes vidéos et, éventuellement les livres. De même les assurances incendie et les assurances vie peuvent être considérées comme des produits analogues, appartenant à la catégorie des assurances* » [896]. Au-delà de ces difficultés qui peuvent se rencontrer au niveau national, les divergences d'interprétation entre les pays sont susceptibles d'aggraver le contentieux et de fragiliser encore davantage la sécurité juridique et de mettre ainsi à mal la confiance des internautes. En tout état de cause, malgré les craintes formulées par la CNIL à l'égard de cette notion, celle-ci souligne qu'aucune difficulté particulière ne s'est posée pour le moment. La raison principale peut résider dans le fait qu'une entreprise de renommée n'a pas d'intérêt à importuner ses clients par des *e-mails* publicitaires qui ne les intéresseraient pas. En effet, cette attitude n'aurait d'autre conséquence que de les détourner de cette dernière. Or, le commerce électronique, et en particulier la prospection commerciale par *e-mail*, occupe aujourd'hui une place stratégique dans le développement des entreprises. Ainsi, toute entreprise qui souhaite mener une prospection « *intelligente et rentable* » selon l'expression déjà empruntée au professeur Jean FRAYSSINET [897], doit impérativement faire « *un usage marketing raisonné des messages*

[894] *Id.*
[895] Avis n° 5/2004, avis préc., spéc. p. 10.
[896] De façon identique, l'Arrêté royal belge du 4 mai 2003 visant à réglementer les envois commerciaux par courrier électronique a prévu un régime d'exception au consentement préalable relatif aux produits analogues. Cette exception est conditionnée par le respect de trois conditions cumulatives. Tout d'abord, le prestataire doit avoir obtenu les coordonnées électroniques à la suite d'une relation commerciale antérieure, mais uniquement pour des produits ou services que lui même fournit (ce qui exclut la communication de telles données à des filiales, sociétés sœurs ou société mère qui sont des personnes juridiques différentes, article 1er alinéa 4). L'exploitation de ces données à des fins publicitaires est limitée exclusivement à des produits ou services analogues à ceux qu'il a initialement vendus à son client, avec toute l'ambiguïté que renferme ce terme. Enfin, le prestataire doit fournir au moment de la collecte la faculté de s'opposer sans frais et de manière simple, à cette exploitation.
[897] V. Jean FRAYSSINET, « Nouvelles technologies de l'information et de la communication et protection des libertés des consommateurs », art. préc., spéc. p. 46.

envoyés pour des " services analogues " » et notamment offrir à ses clients la possibilité d'exercer de façon effective leur droit de s'opposer à toute nouvelle prospection [898].

318. L'identité de « personne physique ou morale ». Le G29, commentant les dispositions de l'article 13.2 de la directive 2002/58/CE, avait précisé que seule la même personne physique ou morale qui avait collecté lors d'une prospection commerciale précédente des adresses électroniques pouvait envoyer de nouveaux *e-mails* commerciaux à ces dernières [899]. Si l'exigence d'identité de personne physique ne pose pas de difficulté d'interprétation, il n'en est pas de même pour les personnes morales. En effet, il convient de déterminer si plusieurs entités peuvent être considérées comme une personne morale unique. En commençant par l'hypothèse la plus simple, il est possible d'exclure d'emblée du champ de cette exception les sociétés qui n'auraient pas, par définition, été impliquées dans la première vente ou prestation de services conclue. Il semble également que celles qui auraient seulement acquis ou loué un fichier de contacts ne soient pas davantage concernées. Quant aux filiales et sociétés mères, le G29 a précisé que cette dérogation ne les concernait pas dans la mesure où ces entités ne sont pas considérées comme la même entreprise [900].

2. L'hypothèse des adresses professionnelles

319. Des précisions à apporter. Selon l'article 22 de la LCEN, le régime de l'*opt-in* est circonscrit aux « *coordonnées d'une personne physique* ». Comme nous l'avons exposé précédemment, la CNIL consacrait une interprétation très stricte du régime français en soumettant au respect du consentement préalable tout prospecteur qui envoyait des *e-mails* publicitaires aux adresses de personnes physiques et ce, quelle que soit la finalité de leur utilisation, personnelle ou professionnelle. Cette position a soulevé le mécontentement général au sein des entreprises de prospection, notamment de la part de la FEVAD et du SNCD qui, dès le mois de mai 2003, dénonçaient cette interprétation comme une menace pour la pérennité de la publicité par voie électronique transmise. Rappelant que son but n'était autre que celui de protéger les consommateurs, la CNIL a ainsi reconsidéré sa position lors de la séance du 17 février 2005 [901]. Tout en maintenant le principe de l'*opt-in* pour la prospection

[898] Sur ce point, v. Jean DIONIS DU SEJOUR et Corinne ERHEL (présenté par), *Rapport d'information sur la mise en application de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique*, rapport préc., spéc. pp. 44-45
[899] Avis n° 5/2004, avis préc., spéc. p. 10.
[900] *Id., loc. cit.*
[901] CNIL, « Position de la CNIL sur la prospection par courrier électronique dans le cadre professionnel », 2 mars 2005, disponible sur : http://www.cnil.fr/es/la-cnil/actu-cnil/article/article/position-de-la-cnil-sur-la-prospection-par-courrier-electronique-dans-le-cadre-professionnel/.

commerciale « B to C » (*Business to Consumer*), elle a en revanche autorisé, dans le cadre de prospections impliquant exclusivement des professionnels (*Businesse to Business*, également désigné « B to B »), l'envoi d'*e-mails* commerciaux à des adresses électroniques professionnelles sans le consentement préalable des intéressés ; les personnes morales conservant toutefois « *dans tous les cas* » un droit d'opposition à recevoir de nouvelles prospections (régime de l'*opt-out*) [902]. Cette tolérance était cependant soumise à la condition que le message leur soit adressé au titre de leur fonction et sous réserve que le contenu du message soit en lien avec leur activité professionnelle [903]. Par ailleurs, la CNIL rappelle que l'adresse électronique utilisée par une personne physique à titre professionnel n'en constitue pas moins une donnée à caractère personnel au sens de la loi IFL. Il en résulte que bien que le principe du consentement préalable soit levé, les règles en matière de protection des données à caractère personnel restent maintenues, en particulier, l'obligation d'information préalable et le droit d'opposition [904]. Cette nouvelle interprétation consacrée par la Commission doit, selon nous, être approuvée dans la mesure où elle répond au souci d'équilibre que s'efforce d'assurer la LCEN depuis ses débuts. En effet, les petites entreprises, qui n'ont que de faibles budgets à consacrer au *marketing* direct, dépendent en grande partie de cette méthode de prospection peu onéreuse pour se faire connaître. Celle-ci ne doit dès lors être ni sacrifiée ni limitée de façon excessive. À l'occasion du rapport de 2009 relatif à la mise en œuvre de la LCEN, les rapporteurs ont d'ailleurs recommandé de « *préciser le régime législatif de la prospection commerciale électronique de professionnel à professionnel, en s'inspirant des décisions prises par la CNIL* » [905].

C. UN VOLET PENAL INEXPLOITE ET D'APPLICATION LIMITEE

320. Des sanctions théoriquement fortes mais d'effectivité limitée. À l'occasion d'une réflexion engagée sur les moyens de lutte anti-*spam*, l'OCDE avait souligné

[902] Art. 22-II, al. 7 loi n° 2004-575 : « *Dans tous les cas, il est interdit d'émettre, à des fins de prospection directe, des messages au moyen d'automates d'appel, télécopieurs et courriers électroniques, sans indiquer de coordonnées valables auxquelles le destinataire puisse utilement transmettre une demande tendant à obtenir que ces communications cessent sans frais autres que ceux liés à la transmission de celle-ci. Il est également interdit de dissimuler l'identité de la personne pour le compte de laquelle la communication est émise et de mentionner un objet sans rapport avec la prestation ou le service proposé* ».

[903] La CNIL rappelle clairement que : « *L'objet de la sollicitation doit également être en rapport avec la profession de la personne démarchée (exemple : message présentant les mérites d'un logiciel à paul.toto@société.fr, directeur informatique)* » (*Rapport d'activité 2005*, rapport préc., spéc. p.71).

[904] Comme le précise la CNIL, l'application des dispositions de la loi IFL conduit à ce que les titulaires de ces adresses se voient « *offrir, de manière expresse et dénuée d'ambiguïté, la possibilité de s'opposer, sans frais, hormis ceux liés à la transmission du refus, et de manière simple, à l'utilisation de ses coordonnées lorsque celles-ci sont recueillies et chaque fois qu'un courrier électronique de prospection est adressé* » (Séance de la CNIL du 17/02/2005, préc.).

[905] *Rapport d'information sur la mise en application de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique*, rapport préc., spéc. pp. 45-46.

l'importance « *de mettre en place un régime de sanctions efficace* » [906]. Elle avait considéré à ce titre que « [l]*a force de la législation dépendra* […] *de la gravité des sanctions et du caractère inéluctable de leur application* » [907] en insistant sur le fait qu'« *il est fondamental que la législation soit respectée, faute de quoi, elle perd toute utilité* » [908]. Aux termes de l'alinéa 2 de l'article R. 10-1 du CPCE, le non-respect du principe du consentement préalable est sanctionné par une amende de 750 euros pour chaque message irrégulièrement expédié. Cette amende s'applique aussi bien à la prospection par courrier électronique qu'à celle réalisée par télécopie ou automate d'appel. En outre, les personnes morales peuvent également être déclarées pénalement responsables des infractions commises par les organes ou représentants ayant agi pour leur compte, le montant de l'amende contraventionnelle s'élevant alors à 3.750 euros. Il apparaît ainsi que l'envoi massif de *spams* peut être, en théorie, lourdement sanctionné. Toutefois, il semble qu'en pratique, son effectivité reste limitée eu égard à la persistance du phénomène du *spamming* et à l'absence, à notre connaissance, de condamnation prononcée sur son fondement. Ce constat peut s'expliquer principalement par le fait que l'objectif premier du « spammeur » est de toucher un public le plus large possible. Lors d'une opération de *spamming*, chaque destinataire considéré individuellement ne recevra, le plus souvent, qu'un seul *spam* provenant de ce « spammeur ». La gêne causée par un même « spammeur » est alors tout à fait insignifiante et conduit les victimes à abandonner toute perspective de poursuite.

§ 3. L'ÉCHEC D'UNE LUTTE GLOBALE CONTRE LE *SPAMMING*

321. À l'exclusion de certains *spams* s'ajoute l'exclusion de certaines victimes de *spams*, entrave à une lutte globale. Outre le champ d'application trop restrictif de la Lcen s'agissant des envois commerciaux [909], l'interdiction posée par la LCEN concerne exclusivement l'envoi de prospections électroniques directes à « *toute personne physique qui n'a pas exprimé son consentement préalable à recevoir des prospections directes par ce moyen* » [910]. En application de cette disposition, seules les personnes physiques, destinataires directs de *spams*, peuvent ainsi se plaindre auprès de la CNIL qui sanctionnera elle-même cette pratique ou saisir la juridiction compétente [911]. En revanche, les personnes morales et

[906] OCDE, *Boîte à outils anti-spam de politiques et mesures recommandées*, rapport préc., spéc. p. 10 et p. 28.
[907] *Id.*, spéc., p. 9 et p. 27.
[908] *Id.*, spéc., p. 10 et p. 28.
[909] Sur cette critique, v. *supra* : n[os] 300 à 302.
[910] Art. 22, al. 2 loi n° 2004-575.
[911] Selon l'article 34-5, al. 6 du CPCE, « *La Commission nationale de l'informatique et des libertés veille, pour ce qui concerne la prospection directe utilisant les coordonnées d'une personne physique, au respect des*

les FAI ne peuvent agir sur le fondement de la LCEN alors même qu'ils sont ceux qui auraient le plus grand intérêt à l'invoquer et surtout, les plus grandes chances d'obtenir le prononcé de sanctions fortes eu égard au nombre de *spams* reçus et donc dissuasives pour le « spammeur ». Tel est par exemple le cas d'une entreprise ou d'un FAI qui serait la cible d'un « spammeur » mal intentionné qui souhaite lui nuire en paralysant le service de messagerie de la première ou en saturant le réseau du second. Cette restriction du champ d'application de la LCEN apparaît dès lors incontestablement inadaptée à une lutte globale contre le *spamming* et à une protection efficace de l'ensemble des « spammés ». Pour mettre fin à cette différence de traitement, l'Association des fournisseurs d'accès et de services Internet (« AFA ») avait proposé, au moment où la LCEN était débattue au Parlement, que ce droit d'agir soit étendu aux FAI au nom de leurs clients. Cette proposition faisait écho à une recommandation formulée dans la Boîte à outils anti-*spam* de l'OCDE de 2006 selon laquelle : « *les FAI doivent être capables de prendre des mesures de protection équilibrées et appropriées pour leurs réseaux, et doivent être autorisés à engager des poursuites contre les spammeurs* » [912]. Néanmoins, la proposition de l'AFA avait été finalement rejetée par le Parlement français. Pour autant, il est incontestable qu'admettre une voie d'action aux fournisseurs marquerait une avancée significative dans la lutte anti-*spam*. On rejoint ainsi la position de l'Assemblée nationale française qui, dans un rapport de 2008, a déclaré l'ouverture de cette voie d'action comme « *indispensable* » dans la mesure notamment où les moyens, et notamment humains, de la CNIL sont limités. [913]. Cette évolution permettrait en effet d'assurer une protection plus large de l'ensemble des « spammés », qu'ils soient directement touchés par la réception de *spams* ou indirectement par le flux massif de *spams* transitant sur leur réseau. À cet égard, il est intéressant de noter que la transposition de la directive 2009/136/CE permettra prochainement de faire évoluer notre droit en ce sens puisqu'aux termes de son considérant 68 il est précisé que : « *Les fournisseurs de services de communications électroniques consacrent des investissements substantiels à la lutte contre les communications commerciales non sollicitées (" pourriels "). Ils sont aussi mieux placés que les utilisateurs finals* [sic] *pour détecter et identifier les polluposteurs, étant donné qu'ils possèdent les connaissances et les ressources nécessaires à cet effet. Les fournisseurs de*

dispositions du présent article en utilisant les compétences qui lui sont reconnues par la loi n° 78-17 du 6 janvier 1978 précitée. À cette fin, elle peut notamment recevoir, par tous moyens, les plaintes relatives aux infractions aux dispositions du présent article ». – La CNIL peut, après avoir reçu les plaintes, dénoncer les « spammeurs » au Parquet, procéder à des avertissements après enquêtes, et prononcer des sanctions pécuniaires (sur le renforcement des pouvoirs de la CNIL, v. art. 44 et s. loi n° 2004-801 du 6 août 2004 (v. *supra*)).

[912] OCDE, *Boîte à outils anti-spam de politiques et mesures recommandées*, rapport préc., spéc. p. 12.

[913] « *Il sera très difficile pour la* [CNIL] *de développer un système d'action construit, recourant tantôt à des sanctions de son propre motif, et tantôt à des actions judiciaires, notamment pour faire apparaître une jurisprudence. En revanche, eu égard aux coûts que la lutte antispam représente pour eux, si les opérateurs acquièrent le droit d'agir en justice au titre des victimes, ils mettront sans hésitation les moyens et le personnel nécessaires pour obtenir des décisions faisant jurisprudence* » (*Rapport d'information sur la mise en application de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique*, rapport préc., spéc. p. 51).

services de messagerie électronique et les autres fournisseurs de services devraient par conséquent avoir la possibilité d'engager des procédures juridiques à l'encontre des polluposteurs, et donc de défendre les intérêts de leurs clients comme faisant partie intégrante de leurs propres intérêts commerciaux légitimes ».

*

* * *

322. L'adoption d'un régime strict d'interdiction du *spamming* reflète la volonté du législateur français de placer l'internaute au cœur du système de protection afin d'assurer au mieux la préservation de son droit à la tranquillité. En assortissant le système de l'*opt-in* d'un régime dérogatoire, le législateur est également parvenu à construire un régime juridique équilibré entre les intérêts privés et le développement du commerce électronique. Dans cette perspective de protection optimale des destinataires d'envois commerciaux, l'essor de nouvelles formes de *spamming*, en particulier les *Blue spams*, imposait de s'interroger sur la compétence de la LCEN à les appréhender au regard des risques tout aussi importants qu'ils font peser sur la tranquillité des internautes. Les évolutions législatives actuelles démontrent que le développement des nouvelles technologies constitue un terrain fertile à la réflexion et que notre système juridique est capable d'évolutions et d'adaptations. Malgré ces avantages, la LCEN ne peut, à elle seule, assurer une lutte globale contre cette pratique. En particulier, il est regrettable de constater d'une part, que même dans les hypothèses de *spamming* couvertes par la LCEN, cette dernière n'a pas réussi jusqu'à ce jour à s'imposer comme un fondement d'action effectif et d'autre part, qu'elle permet aux seules personnes physiques d'agir sur son fondement et prive les victimes les plus gravement atteintes par les effets du *spamming* du bénéfice de sa protection. Au-delà de l'ensemble de ces imperfections, son effectivité risque également d'être mise à mal dans un contexte international en raison de l'existence de lois étrangères autorisant par principe cette pratique, comme c'est le cas aux États-Unis, premier pays émetteur d*e spams.*

SECTION II. AUX ÉTATS-UNIS, UNE AUTORISATION DE PRINCIPE

323. Une série de propositions de lois avortée. En l'absence de législation uniforme en matière de *spamming*, le législateur américain a, dans un premier temps, tenté de lutter contre cette pratique en proposant de recourir aux lois déjà en vigueur et notamment au *Telephone Consumer Protection Act* de 1991 qui prohibait la prospection non sollicitée par voie de télécopies (*junk faxes*) [914]. Toutefois, le *spamming* ne pouvant s'analyser strictement comme des *junk faxes*, les dispositions de la loi de 1991 se sont rapidement révélées insuffisantes, et s'imposait la mise en place d'une législation anti-*spam* fédérale destinée à régir spécifiquement cette pratique. À cette fin, plusieurs sénateurs ont introduit une série de propositions de lois entre 1997 et 2003 lors des 105e (1997-1998 [915]) [916], 106e (1999-2000) [917], 107e (2001-2002) [918] et 108e Congrès (2003-2004) [919], dont nous verrons par la

[914] 47 *U. S. C* 227(b) (1) (C). – V. par ex., Credence E. FOGO, " The Postman Always Rings 4,000 Times : New approaches to Curb Spam? ", 18 *J. Marshall J. of Comp. & Info. L.* 915 (2000) (favorable à un amendement du *Telephone Consumer Protection Act* permettant de couvrir les sollicitations par *e-mails*). – *Contra* Richard C. BALOUGH, " The Do-Not-Call Registry Model is Not the Answer to Spam ", 22 *J. Marshall J. of Comp. & Info. L.* 79 (2003). – Cindy M. RICE, Comment, " The TCPA : A Justification for the Prohibition on Spam in 2002? ", 3 *N.C.J.L. & Tech.* 375 (2002) (" *While the federal regulation of spam is analogous to the regulation of unsolicited faxes under the TCPA in many ways, simply amending the TCPA to incorporate spam is probably not the most effective method of implementation* " (*id.*, spéc. p. 406). – David E. SORKIN, " Unsolicited Commercial E-Mail and the Telephone Consumer Protection Act of 1991 ", art. préc., spéc. pp. 1012-1016 et pp. 1019-1020 (" [t]*he ordinary, commonly understood meaning of 'telephone facsimile machine' includes neither computers nor electronic mail* " (spéc. p. 1013)).

[915] Par souci de simplification de la lecture, nous avons précisé les dates de déroulement des Congrès en prenant pour référence l'année calendaire. Toutefois, il convient de préciser qu'en réalité chacun des Congrès a lieu entre le 3 janvier d'une année x jusqu'au 3 janvier de l'année x + 2 (par ex., le 105e Congrès s'est déroulé entre le 3 janv. 1997 et le 3 janvier 1999).

[916] Les propositions examinées lors du 105e Congrès ne seront ici que mentionnées, celles-ci étant reprises pour la plupart d'entre elles dans les propositions ultérieures : le *Data Privacy Act of 1997* (H.R. 2368), l'*Unsolicited Commercial Electronic Mail Choice Act of 1997* (S. 771), l'*Electronic Mailbox Protection Act of 1997* (S. 875), le *Nitizens Protection Act* (H.R. 1748), l'*E-Mail User Protection Act of 1998* (H.R. 4124), l'*Anti-Slamming Amendmends Act of 1998* (S. 1618), le *Digital Jamming Act of 1998* (H.R. 4176) (l'ensemble de ces textes sont consultables sur : http://thomas.loc.gov/).

[917] Dix propositions de lois ont été débattues au cours du 106e Congrès sans que l'une d'elles ne soit définitivement adoptée (l'ensemble de ces textes est consultable sur le site *Spam Laws*, disponible sur : http://www.spamlaws.com/federal/summ106.shtml) : l'*Inbox Privacy Act of 1999* (S. 759) avait vocation à réglementer la transmission des *e-mails* commerciaux non sollicités et aurait notamment imposé que ces derniers incluent le nom, l'adresse physique, l'adresse électronique et le numéro de téléphone de l'expéditeur et qu'ils contiennent les informations de routage ainsi que les instructions concernant le mécanisme de désinscription. Les expéditeurs auraient été tenus d'honorer les demandes d'*opt-out*. – L'*Internet Growth and Development Act of 1999* (H.R. 1685) proposait de rendre illégal le fait d'utiliser les services d'un FAI pour envoyer des *e-mails* non solllicités aux clients de ce FAI en violation de ses conditions générales d'utilisation. Cette proposition considérait également comme illégal l'envoi massif d'*e-mails* non sollicités contenant une adresse d'expédition, un nom de domaine ou des informations de routages falsifiés ou encore les messages faisant la promotion de logiciels permettant de falsifier les informations de routage. Cette dernière disposition a également été reprise par l'*Internet Freedom Act* (H.R. 1686) et l'*E-Mail User Protection Act* (H.R. 1910). – Le *Protection Against Scams on Seniors Act of 1999* (H.R. 612) et le *Telemarketing Fraud and Seniors Protection Act* (S. 699) visaient à protéger le public, essentiellement les séniors, contre les opérations de *telemarketing* frauduleuses et autoriseraient la FTC à réglementer « *l'amorce, la transmission et la réception* » des *e-mails* commerciaux non sollicités. – Les autres propositions ont été à nouveau présentées lors des autres Congrès : le *Netizens Protection Act of 1999* (H.R. 3024), le *Wireless Telephone Spam Protection Act* (H.R. 5300), le *CAN-SPAM Act* (H.R. 2162), l'*Unsolicited Commercial Electronic Mail Act of 2000* (H.R. 3113), le *Controlling the Assault of Non-Solicited Pornography and Marketing (CAN SPAM) Act of 2000* (S. 2542).

suite qu'elles se rapprochent, pour certaines de leurs dispositions, de la version définitivement adoptée. Toutefois, faute de consensus, aucune de ces propositions n'avait

[918] Huit propositions de loi avaient été introduites lors du 107e Congrès : l'*Anti-Spamming Act of 2001* (H.R. 718) envisageait d'interdire les en-têtes fausses et requerrait de porter une mention pour les messages commerciaux à caractère pornographique. – L'*Anti-Spamming Act of 2001* (H.R. 1017) aurait amendé pour sa part les lois fédérales relatives à la criminalité informatique pour rendre illégal l'envoi *d'e-mails* contenant une adresse d'expédition ou une en-tête fausse. – Le *Controlling the Assault of Non-Solicited Pornography and Marketing (CAN SPAM) Act of 2001/2002* (S. 630) proposait notamment d'imposer une mention précisant le caractère commercial des messages, de préciser des instructions d'*opt-out* et d'interdire les en-têtes trompeuses ou les objets faux contenus dans ces messages. – Le *Netizens Protection Act of 2001* (H.R. 3146), identique à la proposition du même nom introduite en 1999, aurait imposé que les *e-mails* non sollicités contiennent le nom de l'expéditeur, son adresse physique ainsi que son adresse électronique et qu'ils soient accompagnés d'instructions d'*opt-out.* Les objets de messages faux ou trompeurs auraient été interdits pour les *e-mails* envoyés en masse. Ces exigences n'auraient pas supplanté les lois des états gouvernant les *e-mails* commerciaux non sollicités. Les FAI auraient été tenus de notifier à leurs clients leur politique en matière d'*e-mails* non sollicités et auraient dû être capables de poursuivre des clients qui auraient agi en violation des prescriptions légales. – Le *Protection Children From E-Mail Smut Act of 2001* (H.R. 2472) aurait exigé la labellisation des messages à caractère pornographique transmis à des enfants. – Le *Who Is E-Mailing Our Kids Act* (H.R. 1846) aurait sollicité des écoles et des bibliothèques l'adoption de politiques interdisant aux utilisateurs l'envoi d'*e-mails* anonymes *via* leur service. – L'*Unsolicited Commercial Electronic Mail Act of 2001* (H.R. 95), identique à la proposition du même nom présentée lors du 106e Congrès, aurait également imposé la labellisation des *e-mails* commerciaux non sollicités envoyés en masse et aurait interdit le recours à de fausses en-têtes en violation des politiques des FAI si ces dernières ont clairement été mises en ligne sur le site *Web* du FAI. – Enfin, le *Wireless Telephone Spam Protection Act* (H.R. 113) avait vocation à interdire l'utilisation des systèmes de messagerie des téléphones sans fil pour envoyer des publicités non sollicitées (l'ensemble de ces textes est consultable à partir des adresses : http://thomas.loc.gov/ et http://www.spamlaws.com/federal/summ107.shtml).

[919] Lors du 108e Congrès, huit propositions de loi relatives au *spamming* étaient intervenues : l'*Anti-Spam Act of 2003* (H.R. 2515) exigeait que la nature commerciale des *e-mails* soit clairement indiquée, que l'expéditeur fournisse une adresse postale physique valide et qu'il prévoie un mécanisme d'*opt-out*. Par ailleurs, auraient été notamment interdits les *e-mails* commerciaux avec une en-tête fausse ou trompeuse ainsi que les envois vers des adresses générées de façon aléatoire et automatique. – Le *Criminal Spam Act of 2003* (S. 1293), ne s'appliquant qu'à l'envoi de plus 100 messages par heure ou de 1.000 en trente jours ou encore de 10.000 en un an, envisageait d'interdire de recourir à l'ordinateur de tiers sans l'autorisation de ce dernier afin d'expédier massivement des *e-mails* commerciaux, de prohiber le recours à des en-têtes trompeuses et de réglementer l'utilisation des comptes d'*e-mails* ou de noms de domaine multiples destinés à l'envoi massif de tels messages. – Le *Wireless Telephone Spam Protection Act* (H.R. 122) proposait, quant à lui, d'interdire l'utilisation des systèmes de messagerie sur les téléphones sans fil pour envoyer des *spams*. – Selon le *REDUCE Spam Act* (*Restrict and Eliminate the Delivery of Unsolicited Commercial Electronic Mail or Spam Act of* 2003 (H.R. 1933), les *e-mails* commerciaux non sollicités auraient dû inclure une adresse postale physique de l'expéditeur valide, des instructions concernant le mécanisme de désinscription et un label " ADV " (pour " *advertisement* ") et indiquant la nature publicitaire du message ou " ADV : ADLT " (pour " *advertisement for adult* ") destiné à informer que la publicité était réservée à un public adulte en raison de son contenu à caractère pornographique ; ces exigences ne s'appliquant qu'aux messages envoyés dans les mêmes formes à au moins 1.000 adresses électroniques sur une période de deux jours. Enfin, l'envoi de messages contenant des en-têtes ou des objets faux ou trompeurs aurait été prohibé quand bien même l'expéditeur n'aurait pas procédé à des envois massifs. – Le *Stop Pornography and Abusive Marketing Act* (S. 1231) proposait notamment d'exiger de la FTC l'établissement d'un registre " *no spam* "et de consider comme illégal tout envoi d'*e-mails* commerciaux non sollicités à des adresses de cette liste. La FTC aurait été chargée d'interdire l'envoi d'*e-mails* commerciaux à des mineurs même s'ils ne s'étaient pas inscrits sur ce registre. Par ailleurs, l'ensemble de ces messages auraient dû contenir la mention " ADV : " dans leur en-tête ainsi qu'une adresse postale physique de l'expéditeur valide. – Le *Ban on Deceptive Unsolicited Bulk Electronic Mail Act of 2003* (S. 1052) proposait d'interdire l'insertion de fausses informations dans l'en-tête des *e-mails* commerciaux non sollicités, de procéder à la collecte d'adresses électroniques figurant sur les sites *Web* ou sur d'autres sources *via* des logiciels aspirateurs et d'imposer qu'il soit fait mention d'instructions d'*opt-out* et que les demandes d'*opt-out* soient honorées. – Le *Computer Owner's Bill of Rights* (S. 563) aurait imposé pour sa part à la FTC la mise en place d'un registre " *do-not-email* " regroupant les adresses de personnes ou d'entités qui n'auraient pas souhaité recevoir d'*e-mails* commerciaux non sollicités. La FTC aurait été habilitée à prononcer des amendes civiles contre les expéditeurs de tels messages à des adresses listées dans ce registre. – Le *Reduction in Distribution of Spam Act of 2003* (H.R. 2214) proposait d'introduire l'obligation de mentionner le caractère publicitaire des messages et des obligations d'*opt-out* (l'intégralité de ces textes est disponible sur le site *Spam Laws*, accessible à partir de l'adresse *Web* suivante : http://www.spamlaws.com/federal/summ108.shtml).

alors réussi à passer le filtre des deux chambres du Congrès américain [920]. L'échec de ces diverses tentatives pouvait notamment s'expliquer pour des raisons principalement politiques, notamment face à la pression exercée par les sociétés de *marketing* et les médias sur lesquels les membres du Congrès devaient compter pour être réélus. De leur côté, de nombreux États fédérés (trente-six), devançant l'administration fédérale, avaient déjà adopté une législation répressive à l'égard du *spamming*. L'approche retenue par ces différentes lois différait mais se rejoignait autour de deux dispositions majeures : l'interdiction de dissimuler l'identité de l'expéditeur (utilisation de fausses adresses) et celle de falsifier l'origine et le chemin de transmission des *e-mails* non sollicités [921].

324. L'adoption d'une loi fédérale : le *CAN-SPAM Act*. Il a donc fallu attendre que le *spamming* devienne un véritable fléau pour qu'une loi fédérale soit enfin votée. C'est ainsi qu'après un examen minutieux de ses dispositions, le « *Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003* » (ci-après, le *CAN-SPAM Act*) [922] a été déclaré constitutionnel face aux défis du Premier amendement [923] et est entré en vigueur le 1er janvier 2004. La démarche du législateur américain s'est profondément distinguée de celle adoptée en France, centrée sur la protection des destinataires de *spams*. La priorité donnée aux questions d'ordre économique a eu une incidence directe sur le choix du régime adopté en matière d'envois commerciaux. En consacrant le régime de l'*opt-out* qui autorisait par principe tout envoi commercial, l'objectif de la loi américaine était clairement orienté vers la sanction des seuls comportements considérés comme les plus nuisibles. Privilégiant ainsi les intérêts des annonceurs et ceux des entreprises du *marketing direct*, cette loi a été rapidement dénoncée par les utilisateurs de l'internet comme une norme témoignant de très

[920] Pour un aperçu de l'ensemble de ces lois et les causes de leurs échecs, v. not. Gary S. MOOREFIELD, Note, " *SPAM* – It's Not Just for Breakfast anymore : Federal Legislation and the Fight to Free the Internet From Unsolicited Commercial E-Mail ", art. préc. – Sur les législations intervenues entre 1997 et 2003, v. not. David E. SORKIN, " Spam Legislation in the United States ", 22 *J. Marshall J. of Comp. & Info. L.* 3 (2003).

[921] Le Nevada fut le premier État à avoir adopté une loi anti-*spam*, en juillet 1997, suivi de près par l'État de Washington (mars 1998), la Californie (septembre 1998). Une loi anti-*spam* a par la suite été adoptée dans la plupart des États américains : en 1999, le Connecticut, Delaware, l'Illinois, l'Iowa, la Louisiane, la Caroline du Nord, l'Oklahoma, le Tennessee, Rhode Island, la Virginie ; en 2000 : l'Idaho, le Missouri, la Pennsylvanie ; en 2001 : l'Arkansas, le Wisconsin ; en 2002 : le Kansas, le Maryland, le Minnesota, l'Ohio, le Dakota du Sud, l'Utah ; en 2003 : l'Arizona, la Californie, le Colorado, l'Indiana, le Maine, le Nouveau Mexique, le Dakota du Nord, l'Oregon, le Texas, le Woming ; en 2004 : la Floride ; en 2005 : la Georgie. – Pour des détails sur ces lois, v. not. Cathryn LE, Note, " How Have Internet Service Providers Beat Spammers? ", art. préc. – V. ég. Roger Allan FORD, " Preemption of State Spam Laws by the Federal CAN-SPAM Act ", 72 *U. Chi. L. Rev*. 355, spéc. pp. 382–84 (2005). – V. ég. le site de *spamlaws* qui maintient une liste des législations des différents États, disponible sur : http://www.spamlaws.com/state/summary.shtml.

[922] Pub. L. 108-187, Sec. 2, 117 Stat. 2699 (16 déc. 2003) et codifié dans le Code des États-Unis sous la référence 15 *U.S.C.* Sec. 7701-7713 et 18 *U.S.C.* Sec. 1037, disponible sur : http://uscode.house.gov/download/pls/15C103.txt.

[923] Sur la constitutionnalité de la législation anti-*spam* face au Premier amendement, v. *supra* : n° 156 et s. – Sur la constitutionnalité du *CAN-SPAM Act*, v. not. Marc SIMON, Note, " The CAN-SPAM Act of 2003 : Is Congressional Regulation of Unsolicited Commercial E-Mail Constitutional? ", art. préc.

peu de considération à l'égard du droit à la tranquillité des internautes puisqu'elle légalisait une pratique pourtant largement préjudiciable.

325. Une loi controversée. L'adoption du *CAN-SPAM Act* a nécessairement conduit à réorganiser la hiérarchie des normes légales puisqu'en vertu du principe constitutionnel de primauté de la législation fédérale sur les lois des États fédérés (*Preemption of State Laws)* [924], le *CAN-SPAM Act* prime toutes les lois anti-*spam* des États [925]. La supériorité de cette législation fédérale a rapidement divisé l'opinion. Les détracteurs de cette approche affirmaient qu'elle favorisait l'adoption d'un régime moins sévère que celui adopté par certains États fédérés qui assurait une meilleure protection des internautes [926]. Ils la considéraient également comme freinant dangereusement la possibilité de poursuite des « spammeurs », ce qui favorisait la progression du volume de *spams* et réduisait inévitablement la protection accordée aux usagers de l'internet [927]. Au contraire, les partisans du *CAN-SPAM Act* soutenaient que la prépondérance de la législation fédérale offrait l'opportunité de mettre en place une réglementation uniforme et cohérente qui mettait fin à un ensemble de législations des États disparates [928]. Si le *CAN-SPAM Act* primait des lois plus

[924] V. not. Roger Allan FORD, « Preemption of State Spam Laws by the Federal *CAN-SPAM Act* », 72 *U. Chi. L. Rev*. 355, spéc. pp. 363-366 (2005).

[925] Le *CAN-SPAM Act* prime sur toutes les lois d'État régissant spécifiquement l'utilisation du courrier électronique à des fins d'envois de messages commerciaux mais leurs dispositions régissant les fausses indications et les messages trompeurs, y compris les informations attachées à ces messages restent applicables (15 *U.S.C.* 7707 (b) (1)). Par ailleurs, le *CAN-SPAM ACT* ne peut évincer les lois d'État qui sanctionnent les envois au titre d'une autre fraude ou d'un crime informatique (15 *U.S.C.* Sec.7707 (b) (2) (B)).

[926] La législation en Californie par exemple, partisante d'une protection forte des données, avait consacré le régime du consentement préalable. Sur la primauté de la loi fédérale, V. : Roger Allan FORD, " Preemption of State Spam Laws by the Federal CAN-SPAM Act ", art. préc.

[927] Sur les critiques adressées au *CAN- SPAM Act*, v. not. Elizabeth A. ALONGI, Note, " Has the U.S. Canned Spam? ", 46 *Ariz. L. Rev*. 263, spéc. p. 287 et s. (2004). – Vivek ARORA, Note, " The CAN-SPAM Act : An Inadequate Attempt to Deal with a Growing Problem ", 39 *Colum J.L. & Soc. Probs.* 299, spéc. p. 306 et s. (2006) (le *CAN-SPAM Act* n'est pas satisfaisant en raison d'une part, de son champ d'application limité au *spam* commercial, l'auteur proposant ainsi une réglementation des *spams* politiques (*Id.* spéc. pp. 300- 301) et d'autre part, parce que cette loi ne parvient pas à réduire le volume de *spams* de façon suffisante). – Jordan M. BLANKE, " Canned Spam : New State and Federal Legislation Attempts to Put a Lid on It ", 7 *Comp. L. Rev. & Tech. J.* 305, spéc. p. 317 (2004). – R. Jonas GEISSLER, " Whether 'Anti-Spam' Laws Violate The First Amendment ", 2001 *J. Online L*. art. 8, spéc. n° 37 (2001). (" *Spamming can be regulated by private civil actions, by public criminal actions, and by the market place of ideas, without the need for a separate general anti-spam law* "). – Éric GOLDMAN, " Where's the Beef? Dissecting *Spam*'s Purported Harms ", 22 *J. Marshall J. of Comp. & Info. L.* 13, spéc. p. 14 (2003) (la plupart des dommages causés par le *spamming* sont déjà traités de façon adéquate par des lois existantes ou mieux laissés aux solutions de marché). – Daniel L. MAYER, Note, " Attacking a Windmill : Why the CAN-SPAM Act Is a Futile Waste of Time and Money ", 31 *J. Legis*. 177 (2004). – David E. SORKIN, " Spam Legislation in the United States ", art. préc., spéc. p. 11 (" *legislation has had very little impact on spam and CAN-SPAM act of 2003 is unlikely to change the situation* "). – V. ég Jeffrey D. SULLIVAN and Michael B. DE LEEUW, " Spam After CAN-SPAM : How Inconsistent Thinking Has Made a Hash Out of Unsolicited Commercial Email Policy ", 20 *Santa Clara Computer & High. Tech L.J*. 887 (2004). – Lily ZHANG, " CAN-SPAM Act : An Unsufficient Response to the Growing Spam Problem ", 20 *Berkeley Tech. L.J.* 301 (2005).

[928] V. en ce sens, John MAGEE, " The Law Regulating Unsolicited Commercial E-Mail: An International Perspective ", art. préc., spéc. p. 362 (2003) (l'adoption d'une loi fédérale permet de mettre fin à une approche décousue de la régulation du *spamming*. Ce qui est nécessaire est un cadre législatif large et structuré, comprenant une législation fédérale efficace avec un recours continu, mais limité, aux actions civiles privées de

sévères, il n'en demeurait pas moins que le bénéfice de cette loi fédérale était incontestable dans la mesure où la disparité législative ne pouvait assurer une application effective des dispositions, tant en raison de leur nombre – trente-six – que des particularités parfois inconciliables qui pouvaient caractériser certaines dispositions. Désormais, la prospection directe par courrier électronique [929] bénéficiait d'un régime clair et unifié fixant la ligne de conduite à laquelle les sociétés de *marketing direct* pouvaient se référer pour mener leurs activités en toute légalité sur l'ensemble du territoire américain.

326. Champ de l'étude. Par son acronyme « *can spam* », le ton est donné : la loi américaine n'a pas vocation à prohiber la publicité par courrier électronique dans son ensemble mais seulement les pratiques frauduleuses ou trompeuses (§ 1.). La loi américaine, plus pragmatique que la législation française, précise les cas de responsabilité dans certaines hypothèses plus complexes de *spamming* et les sanctions encourues (§ 2.)

§ 1. UNE PROHIBITION LIMITÉE AUX PRATIQUES FRAUDULEUSES OU TROMPEUSES

327. Par principe, le *spamming* est considéré comme licite dès lors que l'internaute n'a pas exprimé son opposition [930], et sous réserve que la personne qui a l'initiative du message [931] et qui fait la promotion de ses produits et/ou services par le biais de ce message [932] respecte une obligation de transparence des envois (A.). Ce principe emporte ainsi l'interdiction de transmettre des messages commerciaux après l'opposition du destinataire (B.). Nous verrons qu'il existe toutefois certaines exceptions au régime de l'*opt-out*, qui ne sont pas sans rappeler celle existantes dans le système français (C.).

droit coutumier). – V. ég. Scot M. GRAYDON, " Much Ado About Spam : Unsolicited Advertising, the Internet and You ", 32 *St. Mary's L.J.* 77 (2000).

[929] Comme la loi française, le champ d'application de la loi anti-*spam* américaine est limité à la nature commerciale des *e-mails*, c'est-à-dire ceux dont l'objet premier est la publicité commerciale ou la promotion d'un produit ou d'un service commercial (15 *U.S.C.* Sec. 7702 (2) (A) : " *The term " commercial electronic mail message " means any electronic mail message the primary purpose of which is the commercial advertisement or promotion of a commercial product or service (including content on an Internet website operated for a commercial purpose)* ". L'attribution du caractère commercial dépendra de la finalité du message. La loi américaine précise que la simple référence à une entité commerciale ou la présence d'un lien renvoyant au site *Web* d'une entité commerciale dans un *e-mail* ne fait pas entrer automatiquement un tel message dans le champ d'application de la loi si la finalité première du message n'est pas commerciale (15 *U.S.C.* Sec. 7702 (2)(D)).

[930] 15 *U.S.C.* Sec. 7704 (a) (4).

[931] 15 *U.S.C.* Sec. 7702 (9).

[932] 15 *U.S.C.* Sec. 7702 (16).

A. L'EXIGENCE DE TRANSPARENCE DES ENVOIS

328. Contenu du message et moyen de transmission. Selon la loi américaine, est prohibé tout envoi de message commercial dont le contenu serait déloyal ou de nature à tromper le destinataire [933]. Outre cette interdiction générale, sont considérées comme illégales l'utilisation de données de transmission fausses ou trompeuses [934] et l'insertion d'une information trompeuse dans l'objet du message en vue d'éveiller la curiosité du destinataire et l'inciter ainsi à l'ouvrir [935]. Ces interdictions visent à sanctionner certaines pratiques auxquelles ont recours les « spammeurs » et qui consistent à dissimuler l'origine du message en utilisant une fausse identité (fausses adresses électroniques ou faux noms de domaine) [936] ou à insérer des en-têtes dont le contenu est destiné à induire en erreur le destinataire [937].

329. La labellisation des messages. Se distinguant de la loi française, le *CAN-SPAM Act* autorise l'envoi de toute communication commerciale non sollicitée dès lors que sa nature publicitaire est clairement précisée dans l'objet ou inclus dans le corps du message [938]. L'objectif de cette disposition est de permettre au destinataire de déterminer rapidement s'il souhaite le lire ou le supprimer. En revanche, les messages à caractère pornographique doivent contenir la mention « *SEXUALLY-EXPLICIT* » dans leur objet afin d'alerter les destinataires, avant leur consultation, de la nature du contenu et leur permettre ainsi de les filtrer plus facilement [939]. La loi précise que la zone immédiatement visible de ce type de message ne doit contenir aucun élément à caractère pornographique, seuls doivent figurer la mention spécifique exigée, l'adresse postale physique valable de l'expéditeur, un mécanisme de désinscription et les instructions permettant d'accéder audit contenu. Eu égard au corps du

[933] 15 *U.S.C.* Sec. 7704 (a) (1). – Notons que c'est la seule disposition qui s'applique indifféremment aux messages électroniques à caractère commercial et à ceux considérés comme *transactional or relationship.*
[934] 15 *U.S.C.* Sec. 7704 (a) (1).
[935] 15 *U.S.C.* Sec. 7704 (a) (2).
[936] Ont ainsi été sanctionnés l'envoi de messages électroniques avec une adresse électronique inexistante dans le champ « *from* », le recours au *spoofing*, la transmission de messages électroniques qui indiquent faussement que le message provient du serveur ou de l'adresse électronique d'un tiers (Pour des illustrations jurisprudentielles de l'ensemble de ces cas, v. FTC, *Effectiveness and Enforcement of CAN-SPAM Act*, rapport préc., spéc. Appendice 1, A-8).
[937] En pratique, cette disposition a été invoquée pour interdire des en-têtes qui indiquaient faussement que le destinataire avait eu une relation antérieure avec l'expéditeur ou que le message provenait du FAI du destinataire ou contenait des informations importantes ou encore dans des cas où l'objet du message contenait des informations qui n'avaient aucun rapport avec le contenu du message (pour des illustrations jurisprudentielles de ces différents cas de figure, v. FTC, , rapport préc., spéc. Appendice 1, A-10).
[938] 15 *U.S.C.* Sec. 7704 (a) (5) (A) (i).
[939] 15 *U.S.C.* Sec. 7704 (d) (1). – Un avis de 2008 de la FTC qui vise à apporter des précisions sur les conditions de mise en œuvre de la loi anti-*spam* explicite l'obligation posée par la disposition 15 *U.S.C.* Sec. 7704 (d) (1). Elle énonce que tout message à caractère pornographique doit contenir la mention : « SEXUALLY-EXPLICIT » (16 *C.F.R.* 316.4).

message lui-même, il ne doit comporter aucune image visible, l'auteur de l'*e-mail* devant créer un lien hypertexte qui donnera la possibilité de la visualiser [940]. Cette disposition est particulièrement judicieuse puisque non seulement elle offre un guide des meilleures pratiques à destination des sociétés de *marketing* direct qui souhaitent exercer leur activité en toute légalité, mais elle renforce aussi la lutte contre le *spamming* en permettant de poursuivre les expéditeurs *d'e-mail* à caractère pornographique sans devoir démontrer que le message électronique ou son contenu constitue une pratique ou un acte trompeur [941].

330. L'interdiction de recourir à des techniques déloyales ou trompeuses comme soutien au *spamming*. La loi américaine interdit l'envoi d'*e-mails* commerciaux à des personnes dont les adresses électroniques ont été collectées sur des sites *Web* au moyen de robots « aspirateurs » sous réserve toutefois que le propriétaire du site ait clairement mentionné que la vente ou le transfert des adresses figurant sur ce site n'était pas autorisé [942]. En France, si une telle précision se révèle en théorie inutile en raison même de l'interdiction générale de collecter des données à caractère personnel sans le consentement préalable du destinataire, la dimension internationale du phénomène la rend sans doute préférable. En effet, ces techniques de collecte automatique ignorant les frontières géographiques des États, les adresses électroniques pourront, en pratique, être aspirées sur tout site *Web*, quelle que soit sa nationalité. Dans ces conditions, il semble que les sites français – et plus largement européens – devront faire figurer cette mention sur leur page d'accueil afin d'éviter que les adresses électroniques qui y apparaissent ne soient collectées par des robots américains. Ainsi, comme le souligne très justement la CNIL, « *cette loi américaine, qui n'avait pourtant pas vocation à avoir des effets extraterritoriaux, les aura de facto pour des raisons techniques* » [943]. Par ailleurs, sont encore interdites les collectes opérées grâce à des logiciels capables de générer automatiquement des adresses, réelles ou non (*dictionary attacks*) [944] ou les techniques consistant à enregistrer de multiples comptes *e-mail* pour envoyer des *spams* de façon dissimulée à partir de ces comptes [945]. Enfin, la loi érige en infraction diverses activités frauduleuses associées au *spam*. Tel est le cas pour tout acte destiné à acheminer ou à relayer des *e-mails* commerciaux par l'intermédiaire de relais ouverts lui permettant ainsi

[940] 15 *U.S.C.* Sec. 7704 (d) (1). Toutefois, ces exigences ne s'appliquent pas si le destinataire a donné son consentement préalable (« *prior affirmative consent* ») à la réception de tel message (15 *U.S.C.* Sec. 7704 (d) (2)) (sur cette exception, v. *infra* : n° 334).
[941] Sur ce point, v. ég. FTC, *Effectiveness and Enforcement of CAN-SPAM Act*, rapport préc., spéc. Appendice 1 A-21 (§ 7).
[942] 15 *U.S.C.* Sec. 7704 (a) (5) (b) (1) (A) (i).
[943] CNIL, *Rapport d'activité 2003*, rapport préc., spéc. p. 69.
[944] 15 *U.S.C.* Sec. 7704 (a) (5) (b) (1) (A). Sur ces pratiques de collecte, V. *supra* : n° 93.
[945] 15 *U.S.C.* Sec. 7704 (a) (5) (b) (2). Précisons que cette disposition ne vise que l'enregistrement des divers comptes et non l'envoi anonyme de messages. La loi érige donc en infraction autonome ces deux types d'actes. Aussi, le « spammeur » qui a utilisé plusieurs comptes à des fins de *spamming* sera ainsi poursuivi sur le fondement de ces deux infractions distinctes.

de déguiser l'origine véritable de l'expéditeur [946]. L'ensemble de ces dispositions participent activement à la lutte contre le *spamming* et ce, malgré l'autorisation de principe gouvernant l'envoi de ce type de message. En effet, si le législateur s'est évertué à ne pas freiner le développement du commerce électronique, l'incrimination des formes les plus agressives de *spamming* permet en pratique d'appréhender un nombre important d'hypothèses de *spamming* dans la mesure où les « spammeurs » ont souvent recours à des logiciels aspirateurs ou à des programmes permettant la génération automatique de ce type de données.

B. L'INTERDICTION D'ENVOI APRES L'OPPOSITION DU DESTINATAIRE

331. Des conditions rigoureuses. Outre l'obligation de préciser clairement la nature publicitaire du message [947], l'expéditeur doit mentionner de façon explicite que le destinataire dispose d'un droit de refuser la réception de nouveaux *e-mails* commerciaux et doit être informé des moyens lui permettant d'exercer cette prérogative [948]. Pour garantir la mise en œuvre de ce droit, la loi exige que l'*e-mail* contienne une adresse électronique valide ou tout autre dispositif similaire lui offrant la possibilité de soumettre sa demande de refus [949]. Elle précise à ce titre que, quel que soit le moyen mis à disposition du destinataire et choisi par ce dernier, celui-ci doit rester opérationnel, c'est-à-dire capable de recevoir de telles demandes, pendant au moins trente jours après la transmission du message initial [950]. L'expéditeur doit également fournir au destinataire une liste à partir de laquelle il pourra choisir quel type de messages il souhaite ou non recevoir de cet expéditeur [951]. Par ailleurs, l'expéditeur ou toute personne agissant pour son compte est tenu de respecter le choix exprimé [952]. Par souci de pragmatisme et d'effectivité, la loi américaine prévoit que l'expéditeur dispose d'un délai de dix jours ouvrables, à compter de la réception de l'opposition, pour prendre en compte la désinscription et stopper tout futur envoi à cette

[946] 15 *U.S.C.* Sec. 7704 (a) (5) (b) **(**3). Pour un exemple de poursuite sur ce fondement, v. FTC, *Effectiveness and Enforcement of Can-Spam Act*, rapport préc., spéc. Appendice 1, A-8.
[947] 15 *U.S.C.* Sec. 7704 (a) (5) (A) (i) préc.
[948]15 *U.S.C.* Sec. 7704 (a) (5) (A) (ii).
[949] 15 *U.S.C.* Sec. 7704 (a) (3) (A) et 15 *U.S.C.* Sec. 7704 (a) (5) (A) (iii). Pour des exemples jurisprudentiels de la violation de cette disposition, v. FTC, *Effectiveness and Enforcement of CAN-SPAM Act*, rapport préc., spéc. Appendices 5, 6 et 7. – La FTC a précisé à cet égard que les boîtes postales et les boîtes aux lettres privées, établies conformément aux règlements de Services Postaux Américains, sont considérées comme satisfaisant les exigences du *CAN-SPAM Act* (16 *C.F.R.* Sec. 316.2 (p)).
[950] 15 *U.S.C.* Sec. 7704 (a) (3) (A) (ii).
[951] 15 *U.S.C.* Sec. 7704 (a) (3) (B).
[952] 15 *U.S.C.* Sec. 7704 (a) (4) (A).

adresse [953]. Toutefois, en cas de problème technique temporaire rendant impossible la réception de messages ou le traitement des demandes, l'expéditeur reste néanmoins tenu de résoudre le problème dans un laps de temps raisonnable [954]. S'agissant de la durée d'efficacité des demandes d'*opt-out*, certains commentateurs de la loi avaient vivement recommandé à la FTC de fixer une date limite au motif qu'en pratique, les listes d'opposition devenaient au fur et à mesure du temps peu lisibles et difficilement gérables. Notant que le Congrès n'avait pas prévu d'imposer un tel délai, ni d'autoriser la FTC à le faire, la Commission a ainsi refusé de répondre positivement à cette demande [955]. Enfin, la FTC a rappelé que les demandes d'*opt-out* doivent être honorées sans condition : le choix de se désabonner ne devant être subordonné ni au paiement de frais supplémentaires, ni à la fourniture d'informations nominatives autres qu'une adresse électronique, ni être soumis à un processus de désabonnement complexe et contraignant [956]. À défaut, les sociétés peuvent être tenues de modifier leur processus de désinscription pour se conformer aux exigences légales [957].

332. Le registre d'*opt-out*. Devant le succès de la « *do not call list* » mise en place par la FTC en juin 2003 et destinée à permettre aux individus de ne pas faire l'objet d'appels téléphoniques à des fins promotionnelles, la FTC disposait d'un délai de six mois à compter de l'entrée en vigueur du *CAN-SPAM ACT* pour étudier la faisabilité et l'effectivité de l'établissement d'un registre semblable, le *Do-Not-E-Mail registry* [958]. Sur la base de l'un de ses rapports réalisé en juin 2004, la FTC avait exprimé de sérieux doutes quant à la pertinence

[953] 15 *U.S.C.* Sec. 7704 (a) (4) (A) (i). – La FTC avait publié le 12 mai 2005 un avis, le *Notice of Proposed Rulemaking* (NPRM), intitulé *Definitions, Implementation, and Reporting Requirements Under the CAN-SPAM Act* (Proposed Rule, 70 *F.R.* 25426, disponible sur : http://www.ftc.gov/os/2005/05/05canspamregformfrn.pdf) qui succédait lui-même à d'autres avis (disponibles sur : http://www.ftc.gov/bcp/edu/microsites/spam/rules.htm et http://www.federalregister.gov) et destiné à clarifier les difficultés que suscitait la mise en application de certaines dispositions du *CAN-SPAM Act*. La FTC a ainsi rendu plusieurs rapports et avis portant sur des points précis du *CAN-SPAM Act*, et notamment sur l'obligation de labelliser les messages à caractère pornographique (*Label for E-mail Messages Containing Sexually Oriented Material*, 69 *F.R.* 21024, 19 avril 2004, disponible sur : http://www.ftc.gov/os/2004/04/040413adultemailfinalrule.pdf). Le 21 mai 2008, elle a publié de nouvelles règles destinées à expliciter la mise en œuvre du *CAN-SPAM Act*, intitulées également *Definitions, Implementation, and Reporting Requirements Under the Can-Spam Act* (73 *F.R* 29654) et codifées dans le *Code of Federal Regulations* (*C.F.R.*), 16 *C.F.R.* Part 316, disponible sur : http://www.ftc.gov/os/2008/05/R411008frn.pdf (sur cet avis, v. *infra*). – Pour des précisions apportées en 2010, 16 *C.F.R.* Part 316.2 et 316.3, consulter la page disponible sur : http://www.federalregister.gov/citations/2005/05/12/05-9353/definitions-implementation-and-reporting-requirements-under-the-canspam-act. – Dans le NPRM, la FTC proposait de réduire cette période à trois jours ouvrables. Toutefois, face aux nombreuses critiques qui se sont élevées contre cette proposition, la FTC a décidé de conserver ce délai de dix jours (16 *C.F.R.* Sec. 316.4, 1).

[954] 15 *U.S.C.* Sec. 7704 (a) (3) (C).

[955] 16 *C.F.R.* Sec. 316.4, 2 : "Notably, Congress chose neither to impose such a time limit nor to specifically authorize the Commission to do so at this time. Consequently, the Commission declines to impose a time limit on the duration of an opt-out request ".

[956] 16 *C.F.R.* Sec. 316.5 et note 239.

[957] Cette exigence existait déjà dans le NPRM de 2005.

[958] 15 *U.S.C.* Sec. 7708 (a)

d'un tel projet [959] et avait en particulier mis en exergue les risques résultant de sa mise en œuvre dans la mesure où sa création donnerait l'opportunité aux « spammeurs » d'avoir accès à des millions d'adresses électroniques valides pour poursuivre leurs activités [960].

C. LES EXCEPTIONS AU REGIME DE L'*OPT-OUT*

333. L'existence de relations commerciales antérieures. De façon similaire au système français, la loi américaine dispense du respect des exigences imposées par le régime de l'*opt-out* les envois de messages découlant d'anciennes relations commerciales (« *transactional or relationship messages* » ou « TORMs ») [961]. Plus précisément, cette exception a vocation à s'appliquer à tout message dont le contenu concerne une relation commerciale antérieurement conclue dont l'objectif est de faciliter, compléter ou confirmer une transaction commerciale à laquelle le destinataire a précédemment consenti ou de fournir des informations, notamment sur la garantie ou la sécurité d'un produit commercial acheté ou d'un service utilisé par le destinataire. Il peut également s'agir de messages fournissant une information sur une modification des caractéristiques du produit, une amélioration de ce dernier, ou portant sur un aspect particulier de la relation en cours (une souscription, un compte, un prêt,…). Entrent également dans cette catégorie les messages relatifs à des avantages, des soldes de compte ou informant le destinataire de la livraison prochaine de produits ou de services que le destinataire est en droit de recevoir conformément à une transaction antérieurement conclue avec l'expéditeur [962]. Selon la loi, la FTC peut étendre ou restreindre cette catégorie si cette modification se révèle nécessaire pour s'adapter aux changements de technologies et de pratiques de l'*e-mail* et pour accomplir les objectifs fixés par la loi [963]. Jusqu'à présent, la FTC a refusé d'étendre cette catégorie [964], estimant qu'une

[959] FTC, *National Do Not Email Registry : A Report To Congress*, juin 2004, spéc. p. 23 et s., disponible sur : http://www.ftc.gov/reports/dneregistry/report.pdf. La FTC a en effet clairement conclu à son ineffectivité " *a National Do Not Email Registry in any form would not have any beneficial impact on the spam problem. It is clear, based on spammers' abilities to exploit the structure of the email system, that the development of a practical and effective means of authentication is a necessary tool to fight spam* " (*Id*., spéc. p. 37).

[960] V. en ce sens, Marc SIMON, " The CAN-SPAM Act of 2003: Is Congressional Regulation of Unsolicited Commercial E-Mail Constitutional ? ", art. préc., spéc. pp. 105-106 (qui identifie deux risques : l'un relatif à l'utilisation par les « spammeurs » d'une liste d'adresses valides pour envoyer encore plus de *spams* et l'autre tenant au fait que ce registre prenne rapidement une ampleur très importante avec un nombre croissant d'adresses obsolètes dans la mesure où les internautes changent régulièrement d'adresse électronique). – V. ég. Richard C. BALOUGH, " The Do-Not-Call Registry Model Is Not the Answer to Spam ", art. préc.

[961] 15 *U.S.C.* Sec. 7702 (2) (B) : " *The term " commercial electronic mail message " does not include a transactional or relationship message* ". – La FTC a publié un guide qui fournit un exemple intéressant de ces *e-mails* de ceux dits commerciaux (" The *CAN-SPAM Act* : A Compliance Guide for Business ", sept. 2009, disponible sur : http://www.ftc.gov/bcp/edu/pubs/business/ecommerce/bus61.shtm).

[962] 15 *U.S.C.* Sec. 7702 (17) (A).

[963] 15 *U.S.C.* Sec. 7702 (17) (B).

[964] 16 *C.F.R.* Sec. 316.2 (o).

telle modification ne se justifiait ni au regard des évolutions technologiques ni des objectifs fixés par la loi.

334. Le consentement préalable (l'*opt-in*). Lorsque le destinataire a donné son consentement préalable à la réception d'*e-mails* publicitaires, l'interdiction d'envoyer ce type de messages après une opposition est levée [965]. Tel est le cas lorsque ce dernier a expressément consenti à la réception d'un *e-mail* commercial, soit en réponse à une demande sollicitant un tel consentement, soit de sa propre initiative. Tel est encore le cas lorsque le message provient d'un tiers autre que la personne à qui son consentement a été donné, sous réserve que le destinataire ait clairement été informé, au moment où il a exprimé son accord, que son adresse électronique pouvait être transmise à un tiers à des fins commerciales [966]. Si l'une de ces hypothèses est vérifiée, le message envoyé n'a pas besoin de comporter un label indiquant sa nature publicitaire [967] ou pornographique [968]. En revanche, les autres exigences légales restent applicables, à savoir : la mise en place d'un mécanisme de désabonnement et la communication d'une adresse postale physique valide [969].

§ 2. LES RESPONSABILITÉS ET SANCTIONS

335. Cherchant à anticiper une situation qui permettrait au « spammeur » d'échapper à toute sanction, la loi a défini les personnes considérées comme responsables des envois (A.) et donc susceptibles d'être sanctionnées au titre de violation de la loi anti-*spam* (B.).

A. LES HYPOTHESES DE RESPONSABILITE

336. Le 12 mai 2008, la FTC a publié de nouvelles règles entrées en vigueur le 7 juillet 2008 et destinées à expliciter la mise en œuvre du *CAN-SPAM Act* [970]. Même si cet avis n'a pas de portée contraignante, il constitue un guide précieux pour les entreprises qui entreprendront des campagnes d'*e-mail marketing*. À cet égard, la FTC encourage fortement

[965] 15 *U.S.C.* Sec. 7704 (a) (4) (B).
[966] 15 *U.S.C.* Sec. 7702 (1).
[967] 15 *U.S.C.* Sec. 7704 (a) (5) (B).
[968] 15 *U.S.C.* Sec. 7704 (d) (2).
[969] 15 *U.S.C.* Sec. 7704 (a) (5) (B) *a contrario*.
[970] 16 *C.F.R.* Part 16, préc.

les entreprises à adopter une politique de « *best-practices* » afin d'assurer la conformité de leurs pratiques aux exigences légales. Les nouvelles dispositions de cet avis complètent un processus qui a commencé exactement trois ans auparavant à la suite des diverses questions que soulevaient la mise en œuvre de certaines des dispositions de la loi [971]. La FTC s'est ici attachée à expliciter les solutions applicables dans certaines hypothèses complexes en particulier lorsque l'envoi de *spams* implique le concours de plusieurs expéditeurs. Elle a, dans ce cas de figure, donner les directives permettant de désigner la personne responsable parmi l'ensemble des intervenants (1.). Elle a également contribué non seulement à clarifier le statut des tiers qui interviendraient de façon accessoire dans les envois commerciaux (2.) mais aussi à définir le responsable dans les campagnes de *marketing* recourant à un mécanisme de retransmission (« *forwarding* ») (3.).

1. L'hypothèse des expéditeurs multiples

337. Problématique. Lorsque plusieurs entités sont mises en cause, la FTC propose une méthode permettant d'identifier un expéditeur unique qui sera reconnu comme responsable des envois et tenu, en cette qualité, au respect des obligations fixées par la loi en matière d'envoi commercial [972]. La loi américaine définit l'expéditeur comme la personne à l'origine d'un *e-mail* commercial (initiateur) et qui fait la promotion ou la publicité de son produit, de son service ou de son site *Web* par le biais de ce message [973]. Dans certaines situations, l'identification de l'entité expéditrice peut se révéler délicate, en particulier lorsqu'un message électronique unique fait la publicité de produits ou de services de différentes entités. Tel est le cas par exemple d'une publicité qui ferait la promotion de services d'une agence de tourisme incluant à la fois des annonces pour des hôtels, des compagnies aériennes et des sociétés de voiture de location. Dans cette configuration, en l'absence de règles spécifiques, chacune de ces entités pourrait être tenue de respecter les

[971] Avant cet avis la FTC avait en effet publié, le 12 mai 2005, le *Notice of Proposed Rulemaking* (NPRM) (v. *supra* : note 954).

[972] Pour mémoire, les obligations sont le suivantes : l'interdiction d'envoyer des messages contenant des informations de transmission fausses ou trompeuses (15 *U.S.C.* Sec. 7704 (a) (1)) ou des messages dont l'objet est faux ou trompeur (15 *U.S.C.* Sec. 7704 (a) (2)), l'obligation d'inclure une adresse de retour valide ou tout autre mécanisme équivalent permettant de se désabonner (15 *U.S.C.* Sec. 7704 (a) (3)), l'obligation d'identifier clairement la nature publicitaire du message (15 *U.S.C.* Sec. 7704 (a) (5) (A) (i)) et de notifier explicitement la possibilité de refuser la réception de nouveaux messages commerciaux de cet expéditeur (15 *U.S.C.* Sec. 7704 (a) (5) (A) (ii)) et enfin l'obligation de communiquer une adresse postale physique valide (15 *U.S.C.* Sec. 7704 (a) (5) (A) (iii)). Par ailleurs, tout message à caractère pornographique doit contenir une mention explicite de la nature du message (15 *U.S.C.* Sec. 7704 (d) (1)) et inclure dans l'objet du message les dix-neuf caractères suivants : « *SEXUALLY EXPLICIT* » (16 *C.F.R.* 316.4).

[973] 15 *U.S.C.* Sec. 7702 (16) (A).

exigences incombant à tout expéditeur, ce qui risquerait en pratique de multiplier et de complexifier les actions en responsabilité.

338. La définition d'« expéditeur » revisitée. Afin de clarifier le régime de responsabilité, la FTC avait, dans son avis du 12 mai 2005, proposé une norme complexe pour déterminer qui, parmi un groupe d'annonceurs, supporterait les obligations découlant du statut d'expéditeur. Conservant la définition de l'expéditeur fixée par le *CAN-SPAM Act*, elle avait ainsi attribué à chacun le statut d'expéditeur. Toutefois, par exception, une personne unique pouvait devenir le seul expéditeur au sens de la loi dès lors que cette personne répondait l'un des critères suivants : soit elle initiait la création du message et était chargée d'en contrôler le contenu, soit c'est elle qui déterminait les adresses électroniques auxquelles serait envoyé le message, soit elle était identifiée dans le champ « *from* » comme l'expéditeur du message [974]. Estimée trop vague, cette définition s'était heurtée à un certain nombre de critiques de la part des commentateurs dans la mesure où plusieurs entités pouvaient contribuer au contenu du message électronique et/ou participer à la détermination de la liste d'adresses d'expédition. Par souci de pragmatisme, la FTC a donc simplifié cette définition en retenant que l'expéditeur au sens de la loi serait celui qui initie l'*e-mail* faisant la promotion de ses propres produits ou services et qui est le seul à être identifié dans le champ « *from* » du message [975]. Grâce à cette nouvelle définition, la FTC évacuait ainsi les questions particulièrement complexes tenant à la détermination de la personne qui contrôlait le contenu et qui choisissait les adresses d'expédition des messages. Par ailleurs, en se focalisant sur le seul élément « *from* », cette solution répondait aux attentes des consommateurs qui souhaitaient pouvoir se référer à une règle simple leur permettant d'identifier aisément la personne responsable des envois commerciaux [976].

339. La responsabilité des autres annonceurs. Afin d'éviter que des annonceurs non désignés comme expéditeur du message profitent de cette clause restrictive pour

[974] 70 *F.R.* Sec. 25428 (12 mai 2005).
[975] 16 *C.F.R.* Sec. 316.2 (m) b.
[976] La FTC donne un exemple très éclairant des avantages découlant de la nouvelle définition d'« expéditeur ». À partir de l'hypothèse où plusieurs annonceurs (A, B et C) sont impliqués dans une même campagne de *marketing*. Chacun fait la promotion de ses propres biens ou services dans un *e-mail* unique et a le statut d'expéditeur au sens de la loi. Si c'est le nom de A qui figure dans le champ " *from* " du message, ce dernier sera considéré comme expéditeur tandis que B et C qui contrôlent une partie, voire l'ensemble du contenu du message et/ou fournissent des adresses auxquelles A enverra des *e-mails*, ne seront pas considérés comme des expéditeurs, sauf si A ne respecte pas les obligations à observer en matière d'envois commerciaux (15 *U.S.C.* 7704 (a) (1), 15 *U.S.C. 7704* (a) (2), 15 *U.S.C.* 7704 (a) (3) (A) (i), 15 *U.S.C.* 7704 (a) (5) (A) et 16 *C.F.R.* 316.4, sur ces obligations, v. *supra*). Dans ce cas de figure, un consommateur enverra une demande de désinscription à A, la seule personne identifiée dans le champ " *from* ". À travers cet exemple, on voit que la nouvelle définition d'« expéditeur » présente l'avantage de simplifier considérablement les démarches du destinataire (16 *C.F.R.* Sec. 316.2 (m) b.).

échapper à toute responsabilité, la nouvelle définition introduit une lourde responsabilité pesant sur tous les annonceurs d'une même campagne de *marketing*. Ces derniers sont tenus de s'assurer que l'expéditeur désigné respecte toutes les obligations légales susvisées. À défaut, ils seront considérés comme responsables au même titre que l'expéditeur qu'ils avaient choisi [977].

2. L'intervention accessoire d'un tiers

340. L'intervention d'un fournisseur d'adresses électroniques. La question est de savoir si un tiers dont l'intervention se limite à la fourniture d'une liste d'adresses électroniques à d'autres annonceurs doit honorer les demandes d'*opt-out*. Cette question revient ainsi à déterminer si ce tiers peut satisfaire à la définition d'expéditeur, c'est-à-dire si ce dernier initie le message et fait la promotion de ses produits et/ou services et/ou site *Web* par le biais de ce message [978]. La FTC a estimé que ce tiers n'est pas, par principe, soumis à cette obligation. Dans le cas toutefois où il serait considéré comme « expéditeur » [979], il peut toujours échapper à cette obligation en bénéficiant de la clause restrictive qui permet de désigner un expéditeur unique, conformément à la définition révisée « d'expéditeur » [980].

341. L'intervention d'un affilié. La question de la responsabilité d'un affilié s'insère dans un contexte où ce tiers, en échange d'une contrepartie versée par le vendeur, envoie des *e-mails* destinés à promouvoir le site dudit vendeur grâce à un lien hypertexte dirigeant le destinataire directement sur le site de ce dernier. Dans cette situation, la FTC a considéré que le vendeur qui incite une autre personne, l'affilié, à transmettre des *e-mails* commerciaux pour son propre compte, est considéré comme l'expéditeur au sens de la loi dans la mesure où c'est son produit, son service ou son site *Web* qui est promu dans le message électronique. En revanche, l'affilié devient expéditeur lorsqu'il fait la promotion de son propre produit, service ou site *Web* à l'occasion de la promotion de ceux du commerçant. Dans ce dernier cas, l'un et l'autre devenant expéditeurs, ils peuvent alors désigner parmi eux un expéditeur unique.

3. Le mécanisme du « *Forward-to-a-Friend Email Marketing Campaigns* »

[977] 16 *C.F.R.* Sec. 316.2 (m) b.
[978] V. *supra* : n° 337 et s.
[979] V. *supra* :n° 338.
[980] 16 *C.F.R.* Sec. 316.2 (m) e.

342. Position du problème. Il est des cas où l'expéditeur d'un *e-mail* faisant la promotion de produits et/ou services et/ou sites *Web* d'un vendeur n'est pas le vendeur lui-même mais une des personnes qui en a été destinataire. Le vendeur n'orchestrant pas l'envoi commercial, se pose, dans cette hypothèse, la question de savoir si le vendeur est soumis aux obligations légales incombant à tout expéditeur puisque le message assure la promotion de son activité ou si au contraire, il n'assure qu'un simple transfert du message, auquel cas le *CAN-SPAM Act* n'a pas vocation à s'appliquer. Pour répondre à cette problématique, la Commission a distingué trois situations qu'il convient d'exposer successivement.

343. La question de la responsabilité du vendeur dans le cas où son site *Web* propose un mécanisme de « *forwarding* ». Dans le scénario le plus simple, un site *Web* commercial se limite à fournir un mécanisme permettant au visiteur de faire suivre un *e-mail* faisant la promotion de produits, services ou du site *Web* du vendeur qu'il a reçu, à une autre personne et ce, sans incitation particulière de la part du vendeur, laissant à la seule discrétion du visiteur le choix de l'utiliser. Dans cette hypothèse, la FTC considère que le vendeur assure un simple transport du message, c'est-à-dire ne joue qu'un rôle technique sans être impliqué dans la coordination et le choix des adresses à des fins commerciales [981]. Le vendeur ne sera dès lors pas soumis aux exigences légales en matière d'envois commerciaux [982]. De même, la Commission considère que le vendeur qui se limite à utiliser un langage exhortant les consommateurs à faire suivre un message n'endosse pas le statut d'expéditeur [983]. En revanche, la FTC précise que toute contrepartie versée par la société (offres d'argent, des bons, des remises, des récompenses …) au visiteur de son site, en échange d'une retransmission de son message commercial ou d'une incitation à le faire, dépasse la simple opération de transport du message. Il devra alors respecter les obligations légales qui incombent à tout expéditeur, à savoir notamment la mise en place d'un mécanisme d'*opt-out* ou l'interdiction de transmettre des message à un destinataire qui a fait une demande de désinscription [984].

344. La question de la responsabilité du vendeur en cas d'*e-mails* transmis *via* un programme d'*e-mails* du consommateur. Cette hypothèse conduit à la même analyse que celle précédemment exposée. Quels que soient la contrepartie et son montant (y compris des coupons, des remises ou des frais offerts) offerts en échange de la retransmission d'un

[981] Cette action consiste en un simple acheminement, transmission, traitement ou stockage d'un *e-mail* par le biais d'un procédé technique automatique grâce auquel une autre personne qui a identifié les destinataires ou a fourni les adresses de destinataires, envoie des messages (15 *U.S.C.* Sec. 7702 (15)).
[982] 16 *C.F.R.* 5. (c) i.
[983] *Id.*
[984] *Id.*

message, l'expéditeur initial du message sera considéré comme responsable au regard des dispositions du *CAN-SPAM Act*. Il devra en conséquence s'assurer qu'il ne transmet pas un message à un destinataire qui a préalablement fait une demande d'opposition à toute nouvelle prospection et que le message transmis dispose d'un mécanisme d'*opt-out* [985]. Vraisemblablement, cela signifie aussi que, comme dans le cas précédent, les mots d'encouragement non soutenus par une contrepartie supplémentaire ne seront pas pris en compte.

345. La question de la responsabilité du consommateur faisant suivre un *e-mail* commercial. La Commission précise clairement que les consommateurs qui font suivre des messages publicitaires *via* le mécanisme de *forwarding* du vendeur ou leur propre service de messagerie ne doivent pas tomber sous le coup du *CAN-SPAM Act* [986]. Cette disposition relève en effet du bon sens car dans le cas contraire, toute personne endosserait le statut d'expéditeur dès lors que le message a une finalité commerciale.

B. LES SANCTIONS

346. Contrairement à la LCEN, les particuliers ne disposent pas d'un droit individuel de recours devant les tribunaux, seuls sont autorisés à engager des poursuites à l'encontre des « spammeurs », la FTC, les *Attorneys General* des États ainsi que les FAI [987]. La seule possibilité pour les particuliers est alors de porter plainte auprès de l'*Attorney General* de leur État ou auprès de la FTC qui pourra intenter une action en leur nom. Les sanctions administratives seront appliquées par la FTC, principal organisme d'exécution de la loi (a.). Les poursuites au civil pourront être engagées par un procureur général ou un FAI (b.) tandis que la responsabilité de l'application des dispositions pénales revient au *Department of Justice* (DOJ) [988].

[985] 16 *C.F.R.* 5. C (ii).
[986] 16 *C.F.R.* 5. C.(iii).
[987] Pour une vision d'ensemble des différentes affaires dans lesquelles la FTC, les FAI et les États ont engagé des poursuites pour violation du *CAN-SPAM Act*, v. FTC, *Effectiveness and Enforcement of CAN-SPAM Act*, rapport préc., spéc. Appendice 5 (FTC), Appendice 6 (FAI) et Appendice 7 (États). Il existe également d'autres organismes compétents pour faire appliquer la loi anti-spam américaine, selon l'institution qui sera poursuivie pour violation des dispositions du *CAN-SPAM Act*. Par exemple, s'il s'agit d'une banque américaine, c'est l'*Office of Controller of the Currency* qui sera compétent pour faire appliquer la loi. Si le « spammeur » est un courtier ou un négociant, c'est la *Security and Exchange Commission* qui endossera ce rôle. Enfin, d'autres organismes comme la *Federal Communications Commission*, la *Farm Credit Administration*, le *Secretary of Agriculture* et le *Secretary of Transportation* seront compétents lorsque sera mise en cause la responsabilité d'institutions relevant du secteur de l'économie (15 *U.S.C.* Sec. 7706 (b)).
[988] Pour des exemples de poursuites de « spammeurs » par le DOJ, v. not. FTC, *Effectiveness and Enforcement of CAN-SPAM Act*, rapport préc., spéc. Appendice 1, A-2.

a. Les sanctions administratives

347. Les actions de la FTC. Pour l'essentiel, c'est la FTC qui reçoit les plaintes des particuliers et engagent des poursuites [989] et qui peut rendre des ordonnances administratives dont la violation peut donner lieu à des sanctions pécuniaires pouvant atteindre jusqu'à 11.000 dollars par infraction. Elle peut également dans certains cas être habilitée à enquêter et intenter des poursuites de la même façon que le Département de la Justice [990] et prononcer des injonctions de cesser ces activités de *spamming* [991].

b. Les sanctions civiles

348. Dans le cadre des poursuites au civil, la violation des obligations légales en matière d'envois commerciaux est susceptible de donner lieu à deux types d'actions, l'une appartenant aux États et l'autre aux FAI aboutissant à condamner le « spammeur » au versement de dommages et intérêts.

349. L'action des États. Au sein des États, un *Attorney General* ou un *official* ou une agence d'un État peut intenter une action en justice au nom des résidents de son État qui ont signalé des actes illicites afin de les faire cesser et d'obtenir une indemnisation au nom desdites victimes [992]. Le montant de cette indemnisation est égal au plus élevé des deux montants suivants : la perte financière effectivement supportée par ces résidents victimes ou le montant obtenu à partir de la formule légale qui consiste à multiplier le nombre de violations par un montant ne pouvant excéder 250 dollars, le résultat total étant plafonné à deux millions de dollars [993], sauf lorsque l'expéditeur a tenté de masquer son identité [994]. Par ailleurs, tout agissement illicite réalisé sciemment ou toute violation aggravante – collecte d'adresses illicites par des robots « aspirateurs » (*mail harvesting)*, attaques dictionnaire,

[989] 15 *U.S.C.* Sec. 7706 (a).
[990] FTC, *A Brief Overview of the Federal Trade Commission's Investigative and Law Enforcement Authority*, juillet 2008, disponible sur : http://www.ftc.gov/ogc/brfovrvw.shtm.
[991] 15 *U.S.C.* Sec. 7706 (f) (2). Pour des exemples d'actions de la FTC qui ont abouti à des injonctions permanentes et des réparations, v. FTC,*Effectiveness and Enforcement of CAN-SPAM Act*, rapport préc., spéc. Appendice 1 A-24.
[992] 15 *U.S.C.* Sec. 7706. (f) (1) (A), (B).
[993] 15 *U.S.C.* Sec. 7706. (f) (3) (B) (i), (ii).
[994] 15 *U.S.C.* Sec. 7706. (f) (3) (B).

création automatique de comptes d'*e-mails* ou encore piratage informatique (utilisation de l'ordinateur d'un tiers sans son autorisation (*hacking*) [995] – entraîne le triplement du montant des dommages et intérêts [996].

350. L'action des FAI. Les FAI peuvent également agir en justice pour faire cesser les actes du contrevenant et obtenir le versement d'une indemnité pour les dommages qu'ils subissent [997]. Celle-ci sera chiffrée selon un mode de calcul similaire à la méthode légale précitée : ils pourront prétendre au montant le plus élevé entre les pertes financières qu'ils ont effectivement subies et celui calculé selon la même formule légale, mais le nombre de violations sera ici multiplié par un montant ne pouvant dépasser cette fois 25 dollars par infraction avec un maximum total limité à un million de dollars [998]. Lorsque l'expéditeur a tenté de dissimuler son identité, le montant peut atteindre jusqu'à 100 dollars par message illicite [999] et le plafond d'un million de dollars n'est plus applicable [1000]. Comme pour l'action ouverte aux États, en cas d'agissements volontaires et délibérés ou de violations aggravantes, le montant des indemnités peut être triplé [1001].

351. Si la sanction civile permet de sanctionner un agissement dangereux par des dommages-intérêts, cette sanction reste toutefois insuffisante dans la mesure où il est également essentiel de protéger la société contre de tels agissements. Le droit pénal a donc vocation à intervenir afin de sanctionner tout comportement constituant un danger pour l'ordre social dans son ensemble.

c. Les sanctions pénales

352. Champ d'application et sanctions. Cinq activités de criminalité informatique associées au *spam* sont incriminées sur le fondement de la section intitulée « *Fraud and related activity in connection with electronic mail* » [1002] et correspondent à certaines des techniques exploitées par les « spammeurs », soit pour collecter massivement des adresses électroniques, soit pour transmettre des messages en contournant les filtres anti-*spam* afin

[995] 15 *U.S.C.* Sec. 7704 (b).
[996] 15 *U.S.C.* Sec. 7706 (f) (3) (C) (i), (ii).
[997] 15 *U.S.C.* Sec. 7706 (g) (1) (A), (B).
[998] 15 *U.S.C.* Sec. 7706 (g) (3) (A) (ii), (B).
[999] 15 *U.S.C.* Sec. 7706 (g) (3) (A) (i) qui renvoie au 15 *U.S.C.* Sec. 7704 (a) (1) relatif à l'interdiction de données de transmission fausses ou trompeuses.
[1000] 15 *U.S.C.* Sec. 7706 (g) (3) (B).
[1001] 15 *U.S.C.* Sec. 7706 (g) (3) (C). – Pour des exemples d'actions menées par les FAI, v. : FTC, *Effectiveness and Enforcement of CAN-SPAM Act*, rapport préc., spéc. Appendice 6.
[1002] 15 *U.S.C.* Sec. 7703 et 18 *U.S.C.* Sec. 1037 (a).

d'éviter tout risque que leurs *e-mails* soient détectés comme des *spams* [1003]. Sont ainsi pénalement poursuivis l'envoi massif *d'e-mails* par le biais d'ordinateurs protégés et utilisés sans autorisation et l'utilisation d'un ordinateur protégé pour relayer ce type de messages dans le dessein de tromper les destinataires ou les FAI sur l'origine du message. Est encore pénalement poursuivi le fait de falsifier les informations contenues dans les en-têtes des messages avant leur expédition, l'envoi à partir de faux comptes d'*e-mails* ou de noms de domaines ou encore le fait de se déclarer faussement comme le *registrant* [1004] des adresses IP [1005]. Dans ces hypothèses, les sanctions prononcées sont des amendes et/ou des peines d'emprisonnement pouvant atteindre cinq ans, trois ans ou un an selon la nature de l'infraction [1006].

*

* * *

353. D'un point de vue strictement national, l'adoption du *CAN-SPAM Act* a permis d'unifier la réglementation en matière d'envois commerciaux, ce que ne pouvait assurer la diversité et la désharmonie qui caractérisaient les lois précédant son adoption. Par ailleurs, tout en préservant le développement de la prospection commerciale électronique, l'interdiction des formes les plus agressives de *spamming* et la mise en place d'un régime de responsabilité rigoureusement sanctionné a ainsi permis de contrebalancer le régime d'autorisation consacré. Nonobstant ces points positifs, force est de constater que le système américain ne peut s'imposer comme un instrument de lutte globale contre le *spamming*. En effet, tout comme il l'a été déploré pour le système français, la limitation du champ d'application du *CAN-SPAM Act* aux seuls messages à caractère publicitaire, expose un très grand nombre d'internautes à d'incessantes sollicitations non commerciales, sans que ces derniers ne puissent bénéficier d'un fondement légal de protection.

[1003] Pour des détails sur l'ensemble de ces techniques, v. *supra* : n° 91 et s. et 99 et s.
[1004] V. Glossaire.
[1005] Cette disposition criminalise une technique frauduleuse utilisée par des « spammeurs » qui consiste à obtenir des adresses IP non inscrites sur des listes noires. Pour cela, le « spammeur » se fait passer pour l'entité à qui le bloc d'adresses IP a été transféré ou comme un successeur de cette entité afin de duper l'autorité d'enregistrement des adresses IP et la conduire à transférer les adresses IP convoitées. Grâce à de telles manœuvres, l'envoi de *spams* depuis ces adresses IP permet au « spammeur » d'échapper aux filtres des FAI qui identifient, par erreur, les *spams* comme des *e-mails* légitimes (faux-négatif).
[1006] 18 *U.S.C.* Sec. 1037 (b). – Pour ces actes de criminalité informatique sanctionnés sur le fondement du *CAN-SPAM Act*, v. not. Grant C. YANG, " CAN-SPAM : The First Step to No-Spam ", 4 *Chi-K. J. Intel. Prop.* 1, spéc. p. 5 (2004).

CONCLUSION DU CHAPITRE 2

354. La consécration du régime de l'*opt-in* en droit français témoigne de la volonté du législateur de donner la priorité à la protection des « spammés » et, plus particulièrement à leur droit à être laissés tranquilles. L'analyse de la LCEN a néanmoins révélé plusieurs lacunes qui traduisent une action inachevée. Nous avons pu en effet constater que son champ d'application, cantonné aux courriers électroniques commerciaux, est trop restrictif. Les diverses formes de *spamming* existantes mettent en évidence que cette pratique ne peut en aucun cas se limiter à ces seuls types de message. L'insuffisance de cette loi s'est également confirmée à travers son incapacité à protéger l'ensemble des « spammés », en particulier les FAI alors même que ces derniers comptent sans conteste parmi les victimes de cette pratique.

355. Au-delà de cette analyse centrée sur les dispositions de la loi française, la dimension internationale du *spamming* imposait de s'interroger sur les lois anti-*spam* étrangères puisque l'efficacité de la lutte contre cette pratique dépend nécessairement d'une certaine homogénéité des réponses des divers pays. Or, l'étude comparée des systèmes français et américain nous a permis de constater que leurs réglementations respectives se fondent sur des logiques distinctes, reflet des sentiments ambivalents qu'inspire le *spamming*. Alors que le système français consacre une interdiction générale du *spamming*, le législateur américain, plus soucieux de préserver le développement de la prospection commerciale, limite son interdiction à ses seules formes les plus dangereuses. Toutefois, une étude attentive de ces lois a montré que cette opposition devait être quelque peu nuancée puisque d'une part, les exceptions au régime de l'*opt-in* permettent d'assouplir le principe d'interdiction et d'autre part, l'interdiction des *spams* les plus agressifs en droit américain participent à les réconcilier, au moins partiellement, dans la lutte anti-*spam*. Par ailleurs, cette étude de droit comparé a permis de constater le pragmatisme du système américain à travers l'intervention de la FTC. Les nombreuses précisions qu'elle apporte sur les questions relatives à la responsabilité des « spammeurs » dans les hypothèses de *spamming* les plus complexes facilitent la mise en œuvre du *CAN-SPAM Act* et assurent une plus grande sécurité juridique en évitant les divergences d'interprétation susceptibles de naître entre les juges. Le droit américain fait à cet égard figure d'exemple en matière de méthodologie. Il serait donc intéressant que notre système juridique s'inspire de cette démarche pragmatique, ce qui lui permettrait sans doute de gagner en efficacité. En dépit de ces points positifs, cette bipolarisation persistante des législations risque, comme en matière de protection des données, de compromettre l'efficacité de chacun de ces deux systèmes dans la mesure où le *spamming* sévit le plus fréquemment dans un contexte mondial.

356. L'inefficacité partielle des lois dans un contexte national. Une protection complète des « spammés » impliquait la mise en place d'un système permettant de protéger non seulement les données à caractère personnel contre des collectes et exploitations abusives mais également contre l'envoi de *spams* proprement dit. Cette analyse nous a permis de constater que si dans les textes, le système français apparaît comme un régime très protecteur des droits et libertés des individus, les résultats ne permettent pas en pratique de répondre pleinement aux objectifs poursuivis. D'une part, le volet pénal de la loi IFL souffre d'une inefficacité évidente pour sanctionner les atteintes aux données commises par les « spammeurs » au regard des rares poursuites engagées à leur encontre et des faibles sanctions prononcées. D'autre part, une lutte effective et complète contre le *spamming* est subordonnée à la nécessaire prise en compte de la diversité de cette pratique et à une protection de l'ensemble des « spammés ». Or, la mise en œuvre de la LCEN a révélé les limites de son efficacité au regard de son champ d'application, limité aux seuls *spams* commerciaux mais également parce qu'elle ne pas d'offrir une protection à l'ensemble des victimes. Malgré ce constat quelque peu décevant, nous conclurons l'étude des lois françaises sur une note positive. En effet, l'essor de nouvelles formes de *spamming*, en particulier des *Blue spams*, nous a conduit à évaluer si les lois en vigueur permettaient de répondre aux nouvelles problématiques qui se posaient ou si au contraire, des évolutions étaient souhaitables afin d'offrir des réponses adaptées et pérennes. Les récentes évolutions législatives ont démontré que notre droit est perfectible et peut s'adapter pour répondre à de nouvelles menaces.

357. Le télescopage des lois, frein à l'effectivité d'une lutte *anti-spam* internationale. En raison de la dimension internationale du *spamming*, l'effectivité de la lutte contre cette pratique impose que les différentes législations nationales offrent une protection harmonieuse. Or, la comparaison des systèmes juridiques français et américain a mis en évidence qu'en dépit d'un certain rapprochement, des divergences persistent sur des points importants. S'agissant des rapprochements entre les deux systèmes, l'interdiction des plus agressives de *spamming* par le *CAN-SPAM Act* permet de compenser l'absence de législation générale en matière de protection des données à caractère personnel. En effet, l'interdiction de collecte d'adresses électroniques par aspiration sur les espaces publics de l'internet ou par génération automatique permet de rejoindre à cet égard l'interdiction de collecte déloyale posée par la loi IFL. Quant aux divergences, il convient de relever que, malgré l'interdiction des *spams* les plus dangereux, une forte proportion de *spams* échappe à

tout risque de poursuite et de sanction sur le fondement de la loi anti-*spam* américaine. Cette hétérogénéité laisse pressentir les difficultés qui risquent inexorablement de surgir lorsqu'un « spammeur », autorisé selon sa loi nationale à procéder à l'envoi de *spams,* « bombarderait » les messageries de « spammés » situés dans un autre État qui prohibe cette pratique puisque dans un tel cas de figure, la protection des « spammés » pourrait alors se trouver sérieusement menacée [1007], notamment si la loi désignée comme compétente pour trancher le litige est celle où ce « spammeur » est établi. Tel sera le cas en particulier lorsque des « spammés » français engageraient une action contre un « spammeur » établi aux États-Unis. L'ensemble de ces divergences constitue dès lors une véritable menace pour la protection des « spammés » dans la mesure où elles vont inciter les « spammeurs » à migrer vers des États où la législation en vigueur est plus permissive afin de légitimer plus aisément leur activité.

[1007] Sur les difficultés d'application de la loi nationale dans un contexte international, v. par ex. Jean-Marc COBLENCE, avocat à la cour, qui à l'occasion de l'analyse de certaines dispositions de la LCEN, notamment celles relatives à la publicité, souligne qu'il risque de se poser des « *conflits de juridiction et* [d'] *importants problèmes de lois applicables tels que les traite le droit international privé* » (« Le statut de la publicité dans la LCEN », étude préc., spéc. n° 13).

358. Une protection des « spammés » hautement justifiée. Le publipostage commercial n'est pas une activité nouvelle mais dans sa version électronique, il constitue une forme de démarchage à plus grande échelle offrant l'opportunité de limiter les coûts d'envoi par rapport aux voies de transmission classiques utilisées jusqu'alors (voie postale, télécopie). Victime de son succès, cette méthode de prospection est porteuse de dangers dès lors qu'elle est assimilable au *spamming*. Les adresses électroniques, indispensables à l'existence de cette pratique, font l'objet d'une véritable « traque » de la part des « spammeurs ». Pour mener à bien leur activité, ces derniers n'hésitent pas à recourir à des procédés de collecte illicites à la plus grande inquiétude des titulaires des données qui ont l'impression d'en perdre totalement le contrôle. Cette inquiétude est également alimentée par l'évolution actuelle de cette pratique qui tend vers des agissements dont le niveau d'agressivité ne cesse de progresser. Dans les hypothèses de *spamming* les plus dangereuses, les conséquences peuvent être lourdes pour la victime, seule cible du « spammeur ». La réception massive de *spams* peut, selon la victime touchée, entraîner la saturation de sa boîte électronique ou l'encombrement de la bande passante et la paralysie des services de messagerie électronique. Pour toutes ces raisons, la recherche d'une protection efficace et optimale apparaît pleinement justifiée.

359. Un objectif de protection partiellement manqué. L'insuffisance des réponses offertes par les dispositifs de protection technique exigeait une intervention du législateur pour répondre aux attentes de protection des « spammés ». À cette fin, l'œuvre législative se devait d'être menée sur deux fronts : l'un destiné à protéger les données à caractère personnel, l'autre consacré à l'encadrement des envois de messages. En matière de protection des données à caractère personnel, le législateur français, soucieux de garantir un niveau de protection élevé, a mis en place un encadrement rigoureux des opérations de collecte et de traitement des données, dont la violation expose en théorie le contrevenant à de lourdes sanctions. En pratique cependant, la mise en œuvre de ce dispositif répressif s'est révélée décevante, tant en amont dans sa fonction dissuasive qu'en aval pour sanctionner les agissements illicites des « spammeurs ». S'agissant de la réglementation des envois, le droit français a privilégié la protection des individus contre la réception de messages non sollicités afin de renforcer la confiance des utilisateurs de l'internet, condition *sine qua non* du développement du commerce électronique. Toutefois, le champ d'application trop restrictif de la LCEN apparaît insuffisant pour assurer une protection efficace contre le *spamming*. En effet, comme nous avons pu le voir précédemment, cette pratique ne peut se réduire aux seuls

e-mails non sollicités à caractère commercial. Par ailleurs, la LCEN est apparue incapable d'assurer une protection à l'ensemble des victimes. À ces lacunes, s'ajoutent les difficultés résultant de la dimension internationale du *spamming*. Une lutte anti-*spam* efficace imposait une action harmonieuse des différents États. Or, l'étude comparée des législations française et américaine a clairement mis en évidence que les législateurs avaient ignoré cet impératif, chacun régime national reflétant ce que chaque État entend protéger en priorité. Ces divergences se sont manifestées, tant au regard de la protection des données que de l'encadrement des envois commerciaux. De telles disparités risquent de compromettre l'effectivité de chacune des lois susceptibles de se déclarer compétentes lorsqu'un litige survient dans un contexte international, en particulier lorsque l'une et l'autre aboutissent à des solutions contradictoires. Pour surmonter ces impasses et renforcer la protection des « spammés », le dépassement des lois spéciales s'impose. Pour cela, deux principaux objectifs doivent être atteints. Dans un contexte national, cette voie invite à rechercher d'autres fondements juridiques qui permettraient aux « spammés » d'engager efficacement la responsabilité des « spammeurs ». Dans une perspective internationale, il convient d'emprunter une méthode de raisonnement juridique permettant de résoudre les éventuels conflits qui risquent de naître entre plusieurs lois nationales dans le cas où le *spamming* met en jeu des acteurs de nationalité différente et/ou établis dans différents pays. Tels sont les objectifs qui guideront la prochaine partie de notre analyse.

SECONDE PARTIE

LE DÉPASSEMENT NÉCESSAIRE DE LA PROTECTION SPÉCIALE

360. Les objectifs de l'étude. Afin de pallier aux diverses lacunes des législations spéciales précédemment identifiées, la recherche d'une protection efficace des « spammés » mène nécessairement à interroger d'autres fondements juridiques sur lesquels ces derniers pourraient engager une action contre les « spammeurs ». Pour mener à bien cette recherche, il convient de rappeler, à titre préalable, les objectifs visés. D'une part, le champ de la protection spéciale doit être élargi afin de permettre à l'ensemble des « spammés » de bénéficier d'un régime protecteur. D'autre part, une lutte globale contre le *spamming* impose de prendre en compte l'évolution de cette pratique vers des formes de plus de plus agressives et d'envisager ainsi le(s) fondement(s) juridique(s) qui permettraient d'obtenir la sanction efficace des « spammeurs » et ce, même lorsque leur activité ne relève pas de la sphère commerciale. Enfin, les divers dommages occasionnés aux « spammés » à la suite de la réception de *spams* conduit à rechercher quel(s) fondement(s) juridique(s) leur permettait d'en obtenir la réparation. L'examen des solutions offertes par les différents droits sollicités nous amènera à déterminer dans quelles hypothèses ils pourraient être invoqués de façon pertinente.

361. Les axes de recherche. Pour traiter ces différentes problématiques, il serait vain de suggérer la création d'un droit autonome qui prétendrait pouvoir corriger, à lui-seul, l'ensemble de ces imperfections. Au contraire, nous nous efforcerons de questionner notre droit positif afin d'évaluer sa capacité à appréhender le *spamming* selon l'objectif poursuivi : la sanction des « spammeurs » et/ou l'indemnisation des « spammés ». En effet, les juges nationaux n'ont pas attendu l'adoption d'une loi anti-*spam* pour condamner les « spammeurs ». Nous verrons à ce titre que, si le recours au droit pénal de l'informatique et à la responsabilité civile de droit commun n'était initialement qu'un pis-aller, faute de réponse spécifique au problème du *spamming*, leur vivacité ne peut à ce jour être démentie. Toutefois, l'essor de nouveaux cas de *spamming* nous conduira à envisager des poursuites sur le fondement d'autres droits que ceux qui ont été sollicités au commencement du *spamming*. Nous verrons que malgré des résultats prometteurs du droit positif, son efficacité restera toutefois limitée à un cadre strictement national. Or, dans la plupart des cas, cette pratique présente une dimension internationale, la collecte des adresses, les lieux d'émission et de réception des *spams* pouvant intervenir dans plusieurs États. En raison de cet éparpillement géographique du *spamming*, les juridictions et lois des différents États dans lesquels surviendra au moins une des étapes du processus du *spamming* seront susceptibles de se déclarer compétentes. Dans ces circonstances, des conflits de juridictions et de lois risquent d'être inévitables et de remettre en cause la compétence française.

362. Les objectifs et axes de notre recherche ainsi définis, nous envisagerons tout d'abord dans une perspective nationale, quels droits pourraient permettre d'engager une action en responsabilité efficace contre le « spammeur » (Titre 1.). Une fois, ce *corpus* juridique déterminé, il demeurera essentiel de s'interroger quant à son efficacité dans un contexte international. Plus exactement, il s'agira de déterminer dans quelles hypothèses la loi française et/ou les juridictions françaises pourront être compétentes pour connaître d'un litige entre un « spammeur » et un « spammé » localisé dans des pays distincts. Pour cela, il sera nécessaire d'abandonner tout raisonnement attaché à une logique nationale pour se tourner vers les méthodes proposées par le droit international privé (Titre 2.).

TITRE PREMIER : LA RECHERCHE D'UNE ACTION EN RESPONSABILITÉ EFFICACE CONTRE LES « SPAMMEURS »

363. Des poursuites sur le fondement de la responsabilité pénale seront déclenchées chaque fois que l'objectif recherché sera de sanctionner le « spammeur » pour violation de la loi pénale. À cette fin, nous rechercherons quel droit aura vocation à intervenir dans chacune des différentes hypothèses intéressant notre étude et quelle catégorie de « spammés » pourra utilement l'invoquer. Cette recherche nous permettra ainsi d'évaluer l'efficacité de chacun des fondements répressifs sollicités et d'identifier leurs éventuelles lacunes. Comme nous l'avons exposé précédemment [1008], la réception de *spams* est également susceptible de causer un dommage aux personnes qui en sont destinataires. Outre cette action pénale, le « spammé » pourra également engager la responsabilité civile du « spammeur » afin d'obtenir la réparation du préjudice éprouvé par la réception de *spam.* La mise en œuvre de cette action, dans les divers cas de *spamming* permettra d'apprécier si celle-ci se révèle pleinement efficace ou si au contraire, des évolutions seraient souhaitables.

364. Il convient à présent d'examiner sur quels fondements juridiques la responsabilité pénale (chapitre 1.) et/ou la responsabilité civile (chapitre 2.) du « spammeur » pourra être efficacement engagée.

[1008] V. *supra* : n° 54 et s.

CHAPITRE PREMIER : L'ACTION EN RESPONSABILITÉ PÉNALE

365. L'intérêt de la recherche. Le *spamming* constitue un exemple éloquent des agissements délictueux qui existent sur le réseau. Le droit pénal a vocation à s'appliquer chaque fois que de tels comportements commis sur la toile viennent perturber le tissu social. L'intérêt de s'attacher tout particulièrement à cette pratique se justifie à deux titres. Tout d'abord, les attaques menées par les « spammeurs » contre les systèmes informatiques provoquent leur dysfonctionnement, voire leur paralysie, qui impose la recherche d'une sanction efficace. Par ailleurs, en s'associant à d'autres pratiques illicites, le *spamming* est devenu l'instrument qui facilite leur réalisation. Il convient dès lors examiner sur quels fondements juridiques les « spammés » pourraient engager la responsabilité du « spammeur ». Il s'agira à cette occasion de déterminer leur efficacité en s'attachant à vérifier s'ils peuvent efficacement punir ce dernier et le dissuader de poursuivre son activité. Pour cela, nous envisagerons deux hypothèses : celle où le *spamming* peut être sanctionné directement en tant qu'infraction autonome (Section I.) et celle où il ne peut l'être qu'indirectement dans la mesure où il n'est que le vecteur d'autres infractions (Section II.).

366. Délimitation du champ de l'étude. On dénombre certaines affaires dans lesquelles le *spamming* a été sanctionné au titre de la contrefaçon de marque[1009]. Dans ce cas de figure, le demandeur à l'action est, par hypothèse, le titulaire du signe distinctif en litige qui agit en tant que victime de contrefaçon et non en tant que « spammé » [1010]. L'action en contrefaçon de marque ne rentre donc pas dans le cadre de notre recherche et sera, pour cette raison, exclue de nos prochains développements. C'est cette même raison qui nous conduit à évincer les cas d'usurpation d'identité du champ de notre analyse. En revanche, nous envisagerons l'hypothèse où le « spammeur » a utilisé l'adresse d'un tiers pour envoyer des *spams* et empêcher ainsi toute traçabilité possible du « spammeur » (cas des PC zombies). En effet, dans ce cas, la messagerie de la victime peut se trouver saturée par la réception d'un flot important d'*e-mails* provenant des multiples destinataires mécontents.

[1009] TGI Paris, 3e ch., 18 oct. 2006, *RLDI* mars 2007, n° 25, p. 12 et s., note A. Saint-Martin. – *Propriété industrielle* févr. 2007, comm. 12, p. 30, note P. Tréfigny. – TGI Paris, ord. réf., 6 avr. 2004, *Microsoft c/ E Nov. Developpement.*

[1010] Les *spams* dont le contenu reproduit frauduleusement une marque ne sont pas destinés à être adressés au titulaire de celle-ci mais à de multiples destinataires *lambda.*

SECTION I. LE *SPAMMING*, UNE INFRACTION AUTONOME

367. Le *spamming* saisi par le droit pénal de l'informatique. L'omniprésence de l'informatique dans notre société a multiplié les risques de fraude informatique [1011]. L'importance et l'urgence de protection contre le développement de tels comportements frauduleux [1012] ont conduit le législateur à adopter, dès 1988, une loi spécifique, dite « loi Godfrain » [1013] créant notamment deux types de délit : l'intrusion dans un système de traitement automatisé de données (STAD) et l'entrave au fonctionnement d'un tel système, prévus respectivement aux articles 323-1 et 323-2 du Code pénal [1014]. Ces comportements ne pourront toutefois être poursuivis et sanctionnés sur le fondement de ces dispositions que s'ils s'appliquent à un système de traitement automatisé de données, condition préalable commune à ces délits. Afin d'éviter tout risque d'obsolescence du texte au regard des évolutions rapides de la technique, le législateur a volontairement omis de définir la notion de système [1015]. Nous adopterons donc celle proposée par le Sénat lors des travaux préparatoires de la loi Godfrain à savoir « *tout ensemble composé d'une ou plusieurs unités de traitement, de mémoire, de logiciel, de données, d'organes d'entrées-sorties, et de liaisons, qui concourent à un résultat déterminé* » [1016]. Cette définition est suffisamment large pour englober non seulement le poste du destinataire mais également son système de messagerie. Sans entrer dans un panorama détaillé de tous les types de fraude informatique, nous nous attacherons plus particulièrement à démontrer que le *spamming* peut, dans certaines hypothèses, être sanctionné soit au titre de l'intrusion dans un système (§ 1.), soit

[1011] Sur la notion de fraude informatique, v. Guillaume CHAMPY, « Essai de définition de la fraude informatique », *RRJ* 1988-3, p. 751 et s. – Raymond GASSIN, *Informatique (fraude informatique), Répert. pénal, Dalloz,* oct. 1995, spéc. n[os] 1-2 (expliquant que lorsque le juriste utilise la notion de fraude informatique, il « *ne peut,* […] *que se référer à la loi (aux lois qui, dans son pays, incriminent la " fraude informatique "), que les textes emploient l'expression de manière explicite ou qu'ils utilisent d'autres formulations qui évoquent implicitement celle de " fraude informatique ", comme, par exemple, celles d'atteintes aux systèmes de traitement automatisé de données* »). – La fraude informatique à laquelle font référence nos développements renvoie aux atteintes aux STAD).

[1012] Raymond GASSIN, *Informatique (fraude informatique)*, préc., spéc. n[os] 9-12, p. 4.

[1013] Loi n° 88-19 du 5 janvier 1988 sur la fraude informatique, J.O. du 6 janvier 1988, p. 231 et s. – Sur cette loi, v. not. Henri ALTERMAN et Alain BLOCH, « La fraude informatique », *Gaz. Pal.* 3 sept. 1988, 2, doctr., p. 530 et s. – Françoise CHAMOUX, « La loi sur la fraude informatique : de nouvelles incriminations », *JCP* 1998, éd. G., I. 3321. – Guillaume CHAMPY, *La fraude informatique,* (préf. Gaëtan DI MARINO et avant-propos Jacques GODFRAIN), P.U.A.M., 1992. – Hervé CROZE, « L'apport du droit pénal à la théorie générale du droit de l'informatique (à propos de la loi n° 88-19 du 5 janvier 1988 sur la fraude informatique), *JCP* 1998, éd. G., I. 3333. – Jean DEVEZE, « Commentaire de la loi n° 88-19 du 5 janvier 1988 relative à la fraude informatique », *Lamy Droit de l'informatique,* 1987, mise à jour févr. 1988, p. 3 et s. ; *Atteinte aux systèmes de traitements automatisés, J.-Cl. Pénal Code, Art. 323-1 à 323-7,* spéc. n[os] 22 et s. – Raymond GASSIN, « La protection pénale d'une nouvelle " universalité de fait " en droit français : Les systèmes de traitement automatisé de données (Commentaire de la loi du 5 janvier 1988 relative à la fraude informatique »), *D.* 1989, actu. législ., p. 5 et s.

[1014] Dans un souci d'alléger les développements, nous utiliserons fréquemment le terme « système » pour désigner le « système de traitement automatisé de données » ou encore son acronyme « STAD ».

[1015] Le Code pénal, lui-même, ne s'y est pas hasardé.

[1016] Jacques THYRAUD, Doc. Sénat 1987-1988, 1re session, n° 3, pp. 51-53. – Pour une analyse approfondie de la notion de STAD, v. not. Raymond GASSIN, *Informatique (fraude informatique),* préc., spéc. n[os] 66-76, pp. 12-14. – Raymond GASSIN, « La protection pénale d'une nouvelle " universalité de fait " en droit français : Les systèmes de traitement automatisé de données », art. préc., spéc. n° 55 et s., p. 14 et s.

pour entrave ou perturbation de son fonctionnement (§ 2.). Pour mener à bien cette étude, nous nous attacherons à définir au préalable les éléments constitutifs de chacun de ces délits pour ensuite les transposer au cas de *spamming*.

§ 1. LE *SPAMMING* SANCTIONNÉ POUR INTRUSION DANS UN SYSTÈME

368. Élément légal. L'alinéa 1er de l'article 323-1 du Code pénal incrimine le fait d'accéder ou de se maintenir frauduleusement dans tout ou partie d'un système de traitement automatisé de données. Le délit se décompose donc en deux incriminations distinctes : l'accès et le maintien dans ledit système.

369. Élément matériel : l'accès. La loi ne définit pas l'accès. La jurisprudence a interprété largement cette notion en la définissant comme la pénétration directe ou à distance d'un système, quel que soit le procédé utilisé : « *l'accès frauduleux* […] *au sens de l'article 323-1 du Code pénal, vise tous les modes de pénétration irrégulière d'un système, que l'accédant travaille déjà sur la même machine mais à un autre système, qu'il procède à distance ou qu'il se branche sur une ligne de télécommunication* »[1017]. Pour sa part, la doctrine a généralement consacré une acception large de cette notion, la définissant comme « *l'établissement d'une communication avec le système* »[1018]. L'accès peut notamment résulter d'une manipulation irrégulière par l'insertion d'un cheval de Troie dans un système[1019] ou de l'utilisation du numéro et du code confidentiel d'une carte ou d'une adresse électronique d'une tierce personne, obtenues de façon malhonnête[1020]. Il convient enfin de préciser que ce délit ne suppose pas un accès à l'ensemble du système ; le fait d'atteindre certains logiciels ou certaines bases de données suffit à consommer l'infraction[1021].

[1017] CA Paris, 11e ch., corr., sect. A, 5 avr. 1994, *Assistance Génie Logiciel et Geste c/ Niel et a., Juris-Data* n° 021093 ; *LPA* 5 juill. 1995, n° 80, p. 13 et s., note V. Alvarez ; *JCP* 1995, éd. E., I. 461, n° 20, obs. M. Vivant et C. Le Stanc ; *D.* 1994, I.R., p. 130.

[1018] André LUCAS, Jean DEVEZE, Jean FRAYSSINET, *Droit de l'informatique et de l'Internet, op. cit*., spéc. n° 967, p. 681.

[1019] T. corr. Limoges, 14 mars 1994, *Expertises* 1994, p. 238, obs. Teboul.

[1020] TGI Paris, 12e ch., 26 juin 1995, *France Telecom c/ Dicko, LPA* 1er mars 1996, n° 27, p. 4 et s., note V. Alvarez. – CA Paris, 9e ch. corr., sect. A, 6 déc. 2000, *Juris-Data* n° 134502 ; *Comm. com. électr*. mars 2001, comm. 28, pp. 23-24, obs. C. Le Stanc (fraude à la carte bancaire). – Cass. crim. 3 oct. 2007, pourvoi n° 07-81.045 ; *Bull. crim*., n° 236 ; *D.* 2007, AJ, p. 2807 ; *Rev. sc. crim*. 2008. 99, obs. J. Francillon ; *AJ pénal* 2007, p. 535, obs. G. Royer ; *RTD com*. 2008, p. 433, obs. B. Bouloc ; *Dr. pénal* déc. 2007, comm. 158, pp. 37-38, obs. M. Véron (casse l'arrêt qui relaxe un prévenu du chef de maintien frauduleux dans un système au motif que, même si ce dernier avait accédé régulièrement à une base de données, il avait utilisé pendant plus de deux ans un code d'accès utilisable par les seules personnes autorisées et qui lui avait été remis exclusivement pour une période d'essai).

[1021] Raymond GASSIN, *Informatique (fraude informatique)*, préc., spéc. n° 108. – TGI Paris, 31e ch., 18 sept. 2008, *Éditions Neressis c/ Arkadia, Stéphane V. C*., jugement préc., *Comm. com. électr.* janv. 2009, comm. 10, p.

370. Élément matériel : le maintien. Le maintien peut se définir comme « *l'action de faire durer* » [1022]. Ce dernier peut résulter soit d'un accès régulier, soit d'un accès frauduleux. Le caractère frauduleux du maintien implique de rester connecté alors que le droit d'y accéder a expiré ou n'a jamais existé. L'incrimination du maintien frauduleux présente un grand intérêt lorsque l'accès n'est pas punissable. Tel sera le cas, par exemple, lorsque l'accès est autorisé et par conséquent, non sanctionnable, mais que le maintien dans le système dure au-delà du temps autorisé ou que ce dernier est destiné à prendre copie d'informations alors que leur seule consultation visuelle était autorisée [1023].

371. Élément matériel commun aux deux infractions. La sanction de l'accès, comme celle du maintien, supposent que l'auteur ait pénétré ou demeure dans le système sans aucun droit ni autorisation. À ce titre, la cour d'appel de Paris a jugé que l'accès ou le maintien irrégulier supposait que l'accédant n'ait pas respecté la « *règle du jeu* » [1024]. Cette absence de droit ou d'autorisation peut résulter de la violation d'une disposition légale, d'un contrat ou du non-respect de la volonté du maître du système [1025]. La preuve du caractère frauduleux pourra ainsi résulter du contournement ou de la violation d'un dispositif de sécurité, d'une connexion pirate destinée à interroger à distance un système [1026], de l'introduction d'un fichier espion enregistrant les codes d'accès des abonnés (ver informatique, cheval de Troie, *cookies*, …), etc. [1027]. Précisons enfin que ces deux délits ne sont pas subordonnés à l'exigence d'une limitation préalable de l'accès par un dispositif de protection, « *il suffit que le maître du système ait manifesté son intention d'en restreindre*

48 et s., note É. A. Caprioli (accès à la « *partie confidentielle de la base de données* » d'un site non accessible au public).

[1022] CA Paris, 9e ch. A, 15 déc. 1999, *D.* 2000, I.R., p. 44 ; *Comm. com. électr*. juill.-août 2000, pp. 30-31 ; *Gaz. Pal.* 23 janv. 2001, n° 23, p. 39 et s., note V. Prat (« *le temps qui s'est écoulé* […] *entre le moment de la connexion puis le débranchement de l'appareil* [minitel], *contient en lui-même l'action par les prévenus de faire durer la connexion dans le but avoué d'augmenter la valeur de leur gain* »). – André LUCAS, Jean DEVEZE, Jean FRAYSSINET, *Droit de l'informatique et de l'Internet*, *op. cit*., spéc. n° 968, p. 682.

[1023] V. par ex. T. corr. Brest, 14 mars 1995, *LPA* 28 juin 1995, n° 77, note M.- G. Choisy (caractérise le délit de maintien frauduleux dans un STAD, le fait de procéder, au moyen de vingt-cinq ordinateurs, à la copie de l'annuaire téléphonique de France Telecom afin de les revendre).

[1024] CA Paris, 11e ch. corr., sect. A, 5 avr. 1994, arrêt préc.

[1025] Le maître du système est défini comme « *toute personne physique ou morale, de toute autorité publique, de tout service ou de tout organisme qui est compétent pour disposer du système ou pour décider de sa conception, de son organisation ou de ses finalités* » (v. en ce sens CA Paris, 11e ch. corr., sect. A, 5 avr. 1994, arrêt préc.). – V. ég. en matière de sécurité des systèmes d'information : un administrateur du réseau d'une société a été sanctionné au titre de l'accès frauduleux à des données qui ne lui étaient pas destinées, au motif que ce dernier ne pouvait « *arguer du fait que*, [en cette qualité], *il avait par nature accès à toutes les données, alors que cet accès est limité au besoin de la bonne marche du système et de sa sécurité, et ne peut en aucun cas servir des intérêts qui lui sont personnels* » (TGI Rennes, 21 févr. 2008, *Comm. com. électr*. juin 2008, comm. 8, pp. 45-46, note É. A. Caprioli).

[1026] V. par ex. CA Douai, 4e ch., 7 oct. 1992, *Juris-Data* n° 1992-49432, *JCP* 1994, éd. E., I. 359, spéc. n° 15, obs. M. Vivant et C. Le Stanc (le caractère frauduleux a été déduit de la présence d'une copie d'un logiciel de comptabilité réalisé sans autorisation et permettant d'accéder à des informations sur des tiers).

[1027] V. Christiane FERAL-SCHUHL, *Cyberdroit : Le droit à l'épreuve de l'internet*, 6e éd., *Dalloz*, coll. *Praxis*, 2010, spéc. n° 132.22, p. 915.

l'accès aux seules personnes autorisées » [1028]. Toutefois, en pratique, la mise en place d'un tel dispositif révèlera à l'évidence que l'accès au système et, *a fortiori,* le maintien dans ce système sont limités. La preuve du caractère frauduleux de ces agissements sera ainsi facilitée [1029]. En revanche, il a été jugé que l'accès ou le maintien dans un système ne peuvent être sanctionnés au titre de la fraude informatique lorsqu'ils ont été réalisés par le biais d'un logiciel grand public : « *il ne peut être reproché à un internaute d'accéder aux données ou de se maintenir dans les parties des sites qui peuvent être atteintes par la simple utilisation d'un logiciel grand public de navigation, ces parties de site, qui ne font par définition, l'objet d'aucune protection de la part de l'exploitant du site* […], *devant être réputées non confidentielles à défaut de toute indication contraire et de tout obstacle à l'accès* » [1030].

372. Élément moral : un acte frauduleux volontaire mais sans intention de nuire au système. Les délits d'accès et de maintien frauduleux supposent la volonté de l'agent d'accomplir un acte en ayant conscience de violer la loi pénale [1031]. Le délit d'accès ou de maintien frauduleux suppose donc que les agissements découlent d'un acte volontaire [1032]. La jurisprudence a également considéré que l'accès ou le maintien « *doit être fait sans droit et en connaissance de cause* » [1033], ce qui implique que la personne incriminée

[1028] CA Paris, 11e ch. corr., sect. A, 5 avr. 1994, arrêt préc. – V. ég. en matière de défaçage, TGI Lyon, ch. corr., 27 mai 2008, *Comm. com. électr.* mars 2009, comm. 30, p. 45 et s., note É. A. Caprioli. – Plus récemment, reprenant la motivation de la cour d'appel dans l'arrêt du 5 avril 1994 préc., v. CA Paris, 9 sept. 2009, *Damien B. c/ Forever Living Products France*, *Comm. com. électr.* déc. 2009, comm. 120, pp. 47-49, note É. A. Caprioli. – Hervé CROZE, « L'apport du droit pénal à la théorie générale du droit de l'informatique, doctr. préc., spéc. n° 9. – Philippe JOUGLEUX, « La négligence dans la protection d'un système de traitement automatisé d'informations », *Expertises* 2000, p. 220 et s. – V. ég. Raymond GASSIN, « La protection pénale d'une nouvelle " universalité de fait " en droit français : Les systèmes de traitement automatisé de données », art. préc., spéc. n° 81 et s., p. 19 et s.

[1029] Christiane FERAL-SCHUHL, *Cyberdroit : Le droit à l'épreuve de l'internet*, *op. cit.*, *loc. cit.*

[1030] CA Paris, 12e ch., sect. A, 30 oct. 2002, *Antoine C. c/ Min. pub., Sté Tati*, *Juris-Data* n° 2002-212825 ; *Comm. com. électr.* janv. 2003, comm. 5, pp. 31-32, note L. Grynbaum ; *Expertises*. 2003, n° 266, p 27 et s., note C. Morel. – TGI Paris, 31e ch., 18 sept. 2008, jugement préc. (manipulation au moyen d'un simple navigateur).

[1031] Frédéric DESPORTES et Francis LE GUNEHEC, *ibid.*, *loc. cit.*

[1032] comme le relève la doctrine unanime, v. not. Raymond GASSIN, *Informatique (fraude informatique)*, préc., spéc. n° 131. – Jean DEVEZE, « Commentaire de la loi n° 88-19 du 5 janvier 1988 relative à la fraude informatique », art. préc., spéc. p. 6 *; Atteintes aux systèmes de traitement automatisé de données, J.-Cl. Pénal Code, Art. 323-1 à 323-7*, Fasc. unique, 1997, spéc. n° 39. – Françoise CHAMOUX, « La loi sur la fraude informatique : de nouvelles incriminations », art. préc.. – Hervé CROZE, « L'apport du droit pénal à la théorie générale du droit de l'informatique, doctr. préc., spéc. n° 12. – Guillaume CHAMPY, *La fraude informatique, op. cit.*, tome 1, spéc. p. 236 et s. – André LUCAS, Jean DEVEZE, Jean FRAYSSINET, *Droit de l'informatique et de l'Internet*, *op. cit*., spéc. n° 970, p. 683 (« *Un accès inopiné ou un maintien inconscient ne suraient tomber sous le coup de la loi* »). – Raymond GASSIN, « La protection pénale d'une nouvelle " universalité de fait " en droit français : Les systèmes de traitement automatisé de données », art. préc., spéc. n° 125 et s., p. 28 et s.

[1033] CA Paris, 11e ch. corr., sect. A, 5 avr. 1994, arrêt préc. – CA Paris, 9e ch. A, 15 déc. 1999, arrêt préc. (le fait pour des salariés de se livrer à des jeux sur le minitel de leur employeur caractérise le délit de maintien frauduleux dans un STAD. En l'espèce, ces employés avaient abusivement prolongé leur maintien, durant des heures, voire des nuits entières, hors de leur présence, et à l'insu de leur entourage dans le système – un minitel – grâce aux systèmes d'inhibition et à des écrans noirs donnant l'impression de ne pas être connectés, dans le seul but de multiplier leur nombre de points leur ouvrant droit à des cadeaux).

ait conscience que le maître du fichier ne lui avait donné aucune autorisation [1034]. Il en résulte que l'infraction ne pourra être constituée si l'accès est accidentel ou le maintien est inconscient. La cour d'appel de Paris a en effet jugé que lorsque l'accès à un système de traitement de données était le résultat d'une erreur, « *l'action était dépourvue du caractère intentionnel* » [1035]. En revanche, la loi incrimine « *le maintien irrégulier dans un système de la part de celui qui y serait entré par inadvertance* » [1036] dès lors que ce maintien est volontaire. En effet, le maintien de l'accédant dans le système de façon prolongée, notamment au-delà de la durée autorisée, afin de procéder à diverses opérations participent à la preuve du caractère intentionnel de son intrusion et de sa volonté de se maintenir irrégulièrement dans ledit système. L'intention frauduleuse a pu être caractérisée au regard des moyens utilisés par le contrevenant, en s'attachant notamment à considérer l'effort fourni par l'internaute ainsi que la technicité requise pour accéder à un système. Cette preuve a été établie lorsqu'« *il apparaît* […] *peu probable qu'un internaute muni de simples moyens conventionnels de consultation ait pu accéder à la partie confidentielle de la base de données considérée* » [1037]. Il a ainsi été jugé qu'il n'y a pas d'accès frauduleux dès lors qu'il est possible d'accéder à un serveur par la simple utilisation d'un logiciel grand public de navigation [1038]. En revanche, le caractère frauduleux ne peut être écarté en cas d'accès à un serveur *via* l'utilisation d'un moteur de recherches « *présenté comme à usage professionnel* » et qui « *n'est pas connu du grand public* » [1039].

373. L'indifférence quant aux conséquences engendrées. L'accès et le maintien sont sanctionnés en eux-mêmes, c'est-à-dire indépendamment de l'existence d'un dommage occasionné au système. Il en résulte que l'intention de nuire au système lui-même n'est pas nécessaire pour caractériser ce délit [1040].

[1034] CA Douai, 7 oct. 1992, arrêt préc. – V. ég. CA Paris, 9e ch. corr., sect. A, 6 déc. 2000, arrêt préc. (jugeant que l'élément moral est suffisamment établi aux motifs que « c*ette démarche* […] *inclut la connaissance de la violation de la norme,* [le prévenu]*, qui s'est attaché précisément à forcer les dispositifs de sécurité mis en place, n'ayant pu à aucun moment ignorer au cours de ses années de recherches, elles-mêmes annonées dans ses correspondances* […]*, qu'il accédait dans le STAD du GIE cartes bancaires contre le gré du maître du système* »). – TGI Paris, 1er juill. 2007, *Comm. com. électr.* mars 2008, comm. 46, p. 42 et s., note É. A. Caprioli (« *l'utilisation d'un code d'accès à une messagerie par un ancien salarié constitue bien une manœuvre, l'intéressé ayant parfaitement conscience qu'il n'a plus le droit d'utiliser ce code et ne fait plus partie de la liste des personnes autorisées* »).

[1035] CA Paris, 3e ch., 4 déc. 1992, cité *in* Christiane FERAL-SCHUHL, *Cyberdroit : Le droit à l'épreuve de l'internet*, 6e éd., Praxis Dalloz, 2011/2012, 2010, n° 132.23, p. 833.

[1036] CA Paris, 11e ch. corr., sect. A, 5 avr. 1994, arrêt préc.

[1037] TGI Paris, 31e ch., 18 sept. 2008, jugement préc.

[1038] CA Paris, 12e ch., sect. A, 30 oct. 2002, arrêt préc.

[1039] CA Paris, 9 sept. 2009, arrêt préc.

[1040] V. not. Henri ALTERMAN et Alain BLOCH, « La fraude informatique », art. préc., spéc. p. 532. – Jean DEVEZE, « Commentaire de la loi n° 88-19 du 5 janvier 1988 relative à la fraude informatique », art. préc., spéc. p. 6 ; *Atteintes aux systèmes de traitement automatisé de données*, fasc. préc., spéc. n° 41.– Raymond GASSIN, *Informatique (fraude informatique)*, préc., spéc. n° 132. – André LUCAS, Jean DEVEZE, Jean FRAYSSINET, *Droit de l'informatique et de l'Internet*, *op. cit.*, spéc. n° 971, p. 683.

374. Sanctions. La LCEN [1041] est venue augmenter les sanctions relatives au fait d'accéder ou de se maintenir frauduleusement dans tout ou partie d'un STAD, désormais puni de deux ans d'emprisonnement et de 30.000 euros d'amende [1042]. En cas de dommage, les peines sont alors portées à trois ans d'emprisonnement et 45.000 euros d'amende [1043]. Le dommage peut consister soit en « *la suppression ou la modification des données contenues dans le système* » [1044], soit en « *une altération du fonctionnement de ce système* » [1045] non volontaires [1046] résultant d'une négligence ou d'une imprudence. Enfin, la tentative est punissable au même titre que le délit lui-même [1047].

375. Quid du *spamming* ? Différentes techniques auxquelles le « spammeur » a recours peuvent être poursuivies sur le fondement de l'accès et/ou du maintien dans un système. Tout d'abord, le recours à des PC zombies aux fins d'envoi de *spams* est susceptible de caractériser une fraude informatique au sens de l'article 323-1 du Code pénal. Pour s'en convaincre, il convient de rappeler les deux étapes successives nécessaires à l'accomplissement de cette opération. Dans un premier temps, le « spammeur » doit réussir à prendre le contrôle du poste informatique d'un tiers à son insu, ce qui correspond matériellement à une pénétration sans autorisation dans le système de messagerie d'un tiers. Dans un second temps, il doit se maintenir dans le système suffisamment longtemps pour procéder aux envois. S'agissant de l'élément moral, celui-ci est aisément caractérisé puisque le « spammeur » sait qu'il agit non seulement en violation de la loi pénale, mais aussi que l'accès et le maintien dans le système informatique d'un tiers ne lui sont pas autorisés. Il reste enfin à préciser que, dans cette hypothèse, sa seule volonté est de s'y maintenir le temps de l'envoi des messages, sans que ces agissements n'aient pour dessein d'endommager le système. De même, la technique du *mail bombing* a pu être sanctionnée au titre de l'accès frauduleux à un système. Par un jugement en date du 7 novembre 2003, le tribunal de grande instance du Mans a considéré, à ce titre, que « *l'usage de fausses adresses électroniques d'expéditeur dont certaines ont été usurpées à leur détenteur, ainsi que l'envoi de tels messages sur les services de messageries électroniques de l'entreprise constituent de façon incontestable un moyen frauduleux d'accès dans le système de traitement automatisé gérant*

[1041] Art. 45 loi n° 2004-575. – À l'origine, la sanction s'élevait à un an d'emprisonnement et 100.000 francs d'amende puis, entre le 1er janvier 2002 et jusqu'au 22 juin 2004, elle était fixée à un an d'emprisonnement et 15.000 euros d'amende.
[1042] Art. 323-1 C. pén., al.1er.
[1043] Art. 323-1, al. 2 Code pén.
[1044] Cela rejoint alors l'infraction visée à l'article 323-3 du Code pén. (sur cette infraction, v. *infra* :n° 425 et s.).
[1045] Le terme « altération » correspond alors à l'infraction visée à l'article 323-2 du Code pén. (sur cette infraction, v. *infra* : n° 376 et s.).
[1046] car sinon il y aurait matière à application des articles 323-2 et 323-3 (Jean DEVEZE, *Atteintes aux systèmes de traitement automatisé de données*, fasc. préc., spéc. n° 48).
[1047] Art. 323-7 C. pén. issu de l'art. 46 loi n° 2004-575.

les services de messagerie électronique du groupe » [1048]. Cette décision appelle une remarque. Selon ce jugement, il apparaît que non seulement l'usage de fausses adresses électroniques mais aussi l'envoi de messages caractérisent des moyens d'accéder frauduleusement à un STAD. Or, si le recours à de fausses adresses constitue de toute évidence un moyen d'accéder frauduleusement à un système, il ne peut en être de même s'agissant de l'opération d'envoi d'*e-mails*. En effet, l'envoi de messages n'implique pas nécessairement un accès à un STAD, si tel était le cas, cela reviendrait à considérer comme illicite tout envoi de message, ce qui aurait pour conséquence inévitable de paralyser la communication par voie électronique dans son ensemble [1049]. Il semble que cela n'ait pas été évidemment l'objectif des juges de première instance. Pour revenir à plus d'orthodoxie et interpréter strictement la loi pénale, nous allons voir, qu'à défaut de caractériser un accès frauduleux à un STAD, l'envoi massif de messages peut, dans certains cas, être pénalement sanctionné lorsqu'il provoque une perturbation du fonctionnement d'un système [1050].

§ 2. LE *SPAMMING* SANCTIONNÉ POUR PERTURBATION DU FONCTIONNEMENT D'UN SYSTÈME

376. L'article 323-2 du Code pénal incrimine « *le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données* » [1051]. Cette fraude est le plus souvent commise dans le prolongement d'un accès ou d'un maintien frauduleux [1052] mais elle peut également l'être de façon autonome [1053].

[1048] TGI Mans, ch. corr., 7 nov. 2003, *Sté Smith et Nephew c/ M. L., Gaz. Pal.* 20 juill. 2004, n° 202, p. 44, note É. Barbry. – V. ég. antérieurement TGI Lyon, 1re ch. corr., 20 févr. 2001, *Claranet c/ Patrice C., Comm. com. électr.* janv. 2002, comm. n° 5, p. 28, obs. C. Le Stanc ; *Gaz. Pal.* sept.-oct. 2001, 2, somm., p. 1686, note A. Blanchot (jugeant, de façon expéditive, que l'envoi massif de courriers électroniques a été réalisé « *par suite d'un accès frauduleux* » dans le système informatique de la victime.

[1049] Cela rejoint ainsi les observations d'Alain BLANCHOT (note sous TGI Lyon, 1re ch. corr., 20 févr. 2001, *Gaz. Pal.* sept.-oct. 2001, 2, somm., p. 1686).

[1050] Commentant la décision précitée du 20 février 2001, Alain BLANCHOT souligne, à juste titre, que les agissements auraient dû être sanctionnés au titre de l'entrave au fonctionnement d'un STAD (note préc.).

[1051] Il convient de noter que l'article 323-2, à la différence des articles 323-1 et 323-3 du Code pénal, ne précise pas que l'accès ou le maintien doit être frauduleux. Toutefois, comme le soulignent très clairement André LUCAS, Jean DEVEZE, Jean FRAYSSINET, « *accéder ou se maintenir dans un système, y introduire des données, les modifier ou les supprimer, sont des actes qui en eux-mêmes ne postulent aucune fraude ; il est donc nécessaire que le législateur précise qu'ils ont dû être commis " frauduleusement ". En revanche les termes " altérer " et " fausser" impliquent la violation d'un interdit ; il est donc inutile que la loi précise qu'ils doivent être frauduleux* » (*Droit de l'informatique et de l'Internet, op. cit.*, spéc. n° 974, p. 685).

[1052] V. par ex. TGI Mans, ch. corr., 7 nov. 2003, jugement préc.

[1053] V. not. Cass. crim. 12 déc. 1996, pourvoi n° 95-82198 ; *Juris-Data* n° 005348 ; *Bull. crim.* 1996, n° 465 ; *JCP* 1997, éd. G., IV. 779 ; *RTD com.* 1997, p. 144, obs. B. Bouloc (introduction d'un vírus informatique destructeur dans un logiciel). – Sur l'autonomie de ces deux délits, v. Raymond GASSIN, *Informatique (fraude informatique)*, préc., spéc. n° 161.

377. Élément matériel : l'entrave. L'entrave suppose un acte positif ayant pour objet d'empêcher, de gêner, de ralentir ou de paralyser le fonctionnement du système [1054] dans sa globalité ou de l'un de ses éléments matériels (ordinateurs, périphériques, organe de transmission …) ou immatériels (programmes, données informatives, …) [1055]. L'entrave peut consister en une impossibilité totale d'utiliser le système. Tel est le cas, par exemple, lorsque le prévenu refuse de communiquer les clés d'accès nécessaires pour entrer dans le système [1056]. Tel est le cas encore lorsqu'une bombe logique a été introduite dans un système et a entrainé sa paralysie régulière [1057] ou lors d'une attaque visant à submerger de requêtes un serveur, qui saturé, ne peut plus répondre aux demandes légitimes (déni de service) [1058]. L'entrave peut également résider dans une diminution de la capacité de traitement d'un système. Cette seconde hypothèse correspond à un simple ralentissement de l'activité du système ou à la neutralisation d'une partie de ses fonctionnalités. À cet égard, caractérise le délit d'entrave au fonctionnement des serveurs télématiques l'envoi automatique de messages destinés à « racoler » des utilisateurs pour les détourner vers d'autres serveurs, en recourant à des logiciels de « racolage » qui ont « *eu des effets perturbateurs sur les performances des serveurs et ont entraîné un ralentissement de leur capacité* » [1059]. Toutefois, il convient de préciser que l'infraction ne sera retenue qu'à partir de l'instant où le système est réellement déstabilisé ou altéré dans son activité. C'est donc au fil de la jurisprudence qu'il sera possible de définir plus précisément le niveau de perturbation nécessaire pour que le délit d'entrave soit constitué [1060].

378. Élément matériel : le fait de fausser le fonctionnement. L'action de fausser s'entend comme tout acte ayant pour effet de faire produire au système un résultat différent de celui escompté [1061]. Parmi les multiples procédés utilisés à cette fin, on peut citer les plus

[1054] Sur la notion d'entrave, v. not. André LUCAS, Jean DEVEZE, Jean FRAYSSINET, *Droit de l'informatique et de l'Internet*, *op. cit.*, spéc. n° 973, p. 685. – Raymond GASSIN, « La protection pénale d'une nouvelle " universalité de fait " en droit français : Les systèmes de traitement automatisé de données », art. préc., spéc. n° 157 et s., p. 34 et s.

[1055] Raymond GASSIN, *Informatique (fraude informatique)*, préc., spéc. n° 166.

[1056] CA Paris, 13e ch., 5 oct. 1994 ; *Juris-Data* n° 023667 ; *JCP* 1995, éd. E, I. 461, spéc. n° 21, obs. M. Vivant et C. Le Stanc.

[1057] V. par ex. CA Paris, 9e ch., 15 mars 1994, *Juris-Data* n° 20887 ; *JCP* 1995, éd. E, I. 461, spéc. n° 21, obs. M. Vivant et C. Le Stanc.

[1058] V. par ex., TGI Paris, 12e ch., 19 mai 2006, *Ministère Public c/ Clément P. et al.*, *Gaz. Pal.* 18 janv. 2007, n° 18, p. 35, note J.-F. Forgeron et A. Fiévée, disponible sur : http://www.legalis.net/spip.php?page=jurisprudence-decision&id_article=1714 (attaques destinées à altérer le fonctionnement d'un site Internet par saturation de requêtes, l'une d'elles ayant provoqué la paralysie momentanée des services).

[1059] CA Paris, 11e ch., corr., sect. A, 5 avr. 1994, arrêt préc. – T. corr. Brest, 14 mars 1995, jugement préc. – CA Paris, 9e ch., sect. A, 15 déc. 1999, arrêt préc. (commet le délit d'entrave au fonctionnement d'un STAD la personne qui met en place un système destiné au maintien artificiel d'une communication par minitel).

[1060] Pour un exemple en matière de *spamming*, v. *infra* : n° 381.

[1061] Jean DEVEZE, « Commentaire de la loi n° 88-19 du 5 janvier 1988 relative à la fraude informatique », art. préc., spéc. p. 6 (« *Sous le vocable " fausser ", on peur ranger, non seulement l'insertion de bombe logique ou de cheval de Troie mais encore la fourniture de circuits imprimés permettant de procéder à d'autres opérations que*

classiques tels que les attaques perpétrées par l'intermédiaire d'un virus [1062] ou d'un cheval de Troie influant sur le fonctionnement normal du système, l'insertion d'une bombe logique ou le fait de procéder à des manipulations informatiques afin d'adapter un radiotéléphone au 36-15 [1063].

379. Élément moral. Le délit de l'article 323-2 du Code pénal requiert une volonté de l'agent. Il doit avoir agi avec l'intention de fausser ou d'entraver le système, sans qu'il soit exigé une intention de nuire ou une volonté de causer un dommage [1064]. Il en résulte que si le fonctionnement d'un STAD a été compromis à la suite d'une négligence, d'une imprudence l'auteur des faits échappera à toute poursuite sur ce fondement. En revanche, le délit de l'article 323-2 est constitué dès lors que l'atteinte au fonctionnement du système est volontaire. Faute de toute autre précision, seul un dol général est requis, c'est-à-dire la conscience d'enfreindre la loi pénale [1065]. La preuve de l'intention est le plus souvent déduite des circonstances de l'espèce. Il a été ainsi jugé que l'introduction d'une bombe logique à l'insu des victimes et dans le but de garantir le paiement des redevances de maintenance caractérise l'intention délibérée du prévenu [1066]. Dans une autre affaire, la chambre criminelle de la Cour de cassation a considéré que la cour d'appel avait relaxé à tort les prévenus qui avaient introduit un virus informatique, cette dernière estimant « *qu'il existe un doute sur les circonstances exactes de la contamination de la disquette* ». La Cour de cassation a jugé qu'« [e]*n se bornant à se prononcer ainsi, sans ordonner d'investigations dont elle connaissait la nécessité et dont elle donnait les modalités, et sans répondre aux conclusions des parties civiles faisant valoir que l'intention frauduleuse des prévenus se déduisait de leur parfaite connaissance du diagnostic et des traitements anti-virus, la cour d'appel a violé les articles* [323-2 et 323-3 du Code pénal] » [1067].

380. Sanctions. Comme les délits d'accès et de maintien dans un STAD, la LCEN est venue sanctionner plus sévèrement le fait d'entraver ou de fausser le fonctionnement d'un

celles autorisées et plus généralement toute modification de programme donnant d'autres résultats que ceux attendus ») ; *Atteintes aux systèmes de traitement automatisé de données*, fasc. préc., spéc. n° 58.– André LUCAS, Jean DEVEZE, Jean FRAYSSINET, *Droit de l'informatique et de l'Internet*, *op. cit*., spéc. n° 973, p. 685. – Raymond GASSIN, « La protection pénale d'une nouvelle " universalité de fait " en droit français : Les systèmes de traitement automatisé de données », art. préc., spéc. n° 167 et s., 36 et s.

[1062] Cass. crim. 12 déc. 1996, pourvoi n° 95-82198, arrêt préc.

[1063] CA Paris, 9e ch. A, 18 nov. 1992, *Juris-Data* n° 023257 ; *JCP* 1994, éd. G., I. 359, spéc. n° 15, obs. M. Vivant et C. Le Stanc.

[1064] Jean DEVEZE, *Atteintes aux systèmes de traitement automatisé de données*, fasc. préc., spéc. n° 61.

[1065] Raymond GASSIN, *Informatique (fraude informatique)*, préc., spéc. n° 186. – Jean DEVEZE, *Atteintes aux systèmes de traitement automatisé de données*, fasc. préc., spéc. n° 62 (précisant que si les textes n'exigent pas d'intention, « [s]*ouvent l'intention de nuire – non accessoire – est manifeste : blocage des systèmes pour percevoir le prix de la maintenance, blocage du code d'accès pour discréditer le système* »). .

[1066] CA Paris, 9e ch., 15 mars 1994, arrêt préc.

[1067] Cass. crim. 12 déc. 1996, pourvoi n° 95-82198, arrêt préc.

système de traitement automatisé de données[1068], désormais puni de cinq ans d'emprisonnement et de 75.000 euros d'amende [1069]. La simple tentative est également punissable [1070].

381. Quid du *spamming ?* En matière de *spamming*, l'entrave s'illustre à travers le recours au *mail bombing*, une attaque malicieuse qui consiste à envoyer un afflux d'*e-mails* ciblés à un destinataire, ayant pour effet de ralentir ou de paralyser son serveur de messagerie ou sa bande passante. C'est ainsi, par exemple que le tribunal de grande instance de Nanterre a, par jugement en date du 8 juin 2006, condamné pour entrave au fonctionnement du système informatique d'une société l'envoi de douze mille messages similaires, « *chaque message comportant un sujet généré aléatoirement ainsi qu'un nom d'expéditeur différent, œuvre d'un script automatisé développé pour contourner d'éventuels filtres* » [1071]. Pour sanctionner le prévenu, les magistrats ont jugé que la seule qualification de *mail bombing* suffisait à caractériser ce délit d'entrave [1072], sans préciser en quoi l'élément matériel de ce délit était constitué[1073] alors même que l'envoi massif de *spams* n'est pas automatiquement constitutif d'un délit d'entrave [1074]. S'agissant de l'élément moral, le prévenu, avait tenté, pour sa défense, de se soustraire à sa responsabilité en prétextant, de façon maladroite, qu'il avait « *agi presque par légitime défense* », tout en affirmant qu'il « *n'avait aucune intention de nuire* ». Sans surprise, cette justification n'a pas convaincu les juges nanterrois qui ont constaté que « *son excellente maîtrise des process informatiques s'accommode mal de ses déclarations* » [1075]. Cette décision s'inscrit dans le droit fil d'une précédente affaire jugée pour des faits similaires, et dans laquelle le tribunal de grande instance de Lyon, sans viser

[1068] Art. 45 loi n° 2004-575. – À l'origine, la sanction s'élevait à trois ans d'emprisonnement et 300.000 francs d'amende puis, entre le 1er janvier 2002 et jusqu'au 22 juin 2004, elle était fixée à trois ans d'emprisonnement et 45.0000 euros d'amende.

[1069] Art. 323-2 C. pén.

[1070] Art. 323-7 C. pén. issu de l'art. 46 loi n° 2004-575.

[1071] TGI Nanterre, 8 juin 2006, *Soc Amen c/ Michel M.*, *RLDI* mars 2007, n° 828, p. 46, disponible sur : http://www.legalis.net/jurisprudence-decision.php3?id_article=1868.

[1072] Pour des affaires similaires, v. not. TGI Lyon, 1re ch. corr., 20 févr. 2001, jugement préc. (sans viser expressément l'article 323-2 du Code pénal, le tribunal a condamné pour « *altération du fonctionnement d'un système de traitement automatisé* » le prévenu qui avait envoyé vers le système informatique de son ancien employeur une grande quantité d'*e-mails* vides ainsi que des fichiers de taille importante entraînant la perturbation du système informatique de la société). – TGI Paris, 12e ch., 24 mai 2002, *Lyonnaise Communications c/ M. Philippe P.*, *Comm. com. électr.* juill.-août 2002, actu. 107, p. 4, obs. G. Haas (a été sanctionné sur le fondement de l'article 323-2 du Code pénal un « spammeur » qui, à l'aide d'un logiciel spécialisé, avait procédé à l'envoi de 320.000 messages en une journée bloquant ainsi les serveurs de la société victime pendant une dizaine d'heures les serveurs de l'opérateur).

[1073] Comp. TGI Mans, ch. corr., 7 nov. 2003, jugement préc. (les juges ont constaté que « [l'] *auteur des milliers de messages a réussi à entraver le système de traitement automatisé gérant les services de messagerie électroniques du groupe* […], e*n saturant les boîtes aux lettres électroniques de nombreux destinataires* »).

[1074] V. par ex. CA Paris, 12e ch. B, 18 déc. 2002, *D.* 2002, I.R., p. 940 (prenant le soin de vérifier la réalité de la perturbation du fonctionnement du système, la cour a relaxé un prévenu poursuivi pour *mail bombing* au motif que cette technique n'avait « *pas perturbé de façon sensible le fonctionnement des moyens informatiques mis à la disposition de sa clientèle par la société défenderesse* »). – G. HAAS et O. DE TISSOT, « Le pollupostage non sollicité dans le collimateur de la justice », préc. supra n° 31.

[1075] TGI Nanterre, 8 juin 2006, *Soc Amen c/ Michel M.*, jugement préc.

expressément l'article 323-2 du Code pénal, avait considéré que le prévenu, en qualité de professionnel de l'informatique, avait agi, à titre de représailles, en « *sachant* […] *que les pratiques qu'il allait mettre en œuvre satureraient la bande passante du système* [de son ancien employeur] *et lui causeraient, à brève échéance, le préjudice commercial évidemment recherché* » [1076]. Plus récemment, le tribunal de grande instance du Mans, avait jugé que « [l']*attitude et le mode opératoire utilisé* […] *démontr*[aient] *que l'intéressé* [avait agi] *de façon particulièrement perfide avec une préméditation mûrement réfléchie et dans un but évident de nuire au groupe* » [1077]. Pour conforter sa décision, le tribunal avait considéré que « *l'attitude du prévenu* [était] *manifestement incompatible avec une abolition totale de son discernement, compte tenu de la perception nécessairement excellente de la réalité dont il* [avait] *su faire preuve pour user des travestissements et des stratagèmes précédemment décrits* » [1078]. Le fait de fausser, quant à lui, correspond à l'hypothèse où le « spammeur » a recours à des PC zombies. La prise de contrôle volontaire du poste d'un tiers à son insu aux fins d'envoi de *spams* constitue, de toute évidence, un résultat totalement inattendu et non maîtrisé par la victime. Ce délit peut encore est constitué chaque fois que le « spammeur » envoie des messages contenant des virus puisque cette infection par des *malwares* est souvent destinée à prendre le contrôle du poste informatique victime [1079].

*

* * *

382. À l'issue de cette analyse, il convient de saluer l'œuvre du législateur de 1988 dans laquelle il s'est efforcé de répondre aux risques occasionnés par le développement de l'informatique et qui a su conserver jusqu'à ce jour un dynamisme certain à travers son application au cas de *spamming*. Nous avons en effet constaté que les tribunaux avaient eu l'occasion de sanctionner des « spammeurs » qui s'étaient livrés à des comportements frauduleux tels que le *mail bombing*, ou lorsqu'ils transformaient les postes informatiques en PC zombies. Si ce texte demeure sans conteste toujours d'actualité vingt ans après son entrée en vigueur, il est néanmoins regrettable que sa mise en œuvre par les tribunaux reste trop rare. Malgré le potentiel de ces textes, il convient de noter que les délits d'accès et de maintien fabuleux dans un STAD, comme ceux d'entrave et de perturbation du fonctionnement d'un STAD, permettent de sanctionner les seules formes de *spamming* les

[1076] TGI Lyon, 1re ch. corr., 20 févr. 2001, jugement préc. – Plus récemment, v. TGI Nanterre, 8 juin 2006, jugement préc.
[1077] TGI Mans, ch. corr., 7 nov. 2003, jugement préc.
[1078] *Id.*
[1079] Sur l'association entre le *spamming* et les virus, v. *supra* : n° 104.

plus agressives. Ce constat conduit donc naturellement à rechercher quels instruments répressifs pourraient compléter utilement cet arsenal et venir sanctionner les autres hypothèses de *spamming*.

SECTION II. LE *SPAMMING*, VECTEUR DE MULTIPLES INFRACTIONS

383. La généralisation du recours aux nouvelles technologies a représenté pour les esprits les plus mal attentionnés l'occasion de développer de multiples techniques toujours plus inventives pour commettre des actes délictuels. Face à cette cybercriminalité, l'informatique est devenue un instrument essentiel pour accomplir de multiples délits dont certains, déjà connus du monde réel, seront perpétrés selon des modalités nouvelles. Ce constat s'est notamment vérifié dans de nombreuses hypothèses où le *spamming*, associé à d'autres comportements tout aussi illicites, devient le vecteur d'autres infractions, en facilitant, voire en aggravant leur commission. L'accroissement des interconnexions entre le *spamming* et diverses infractions impose de déterminer, à travers les exemples les plus significatifs, sur quels fondements le « spammeur » pourrait indirectement être poursuivi. À ce titre, nous envisagerons trois hypothèses distinctes : dans les deux premières, les poursuites contre le « spammeur » seront justifiées en raison du contenu des messages reçus [1080], c'est-à-dire, lorsque le *spamming* véhicule des infractions de droit commun, en particulier, l'escroquerie [1081] (§ 1.) ou lorsqu'il participe à la commission d'infractions issues du droit pénal de la consommation (§ 2.). À ces deux hypothèses, s'ajoutera enfin le cas où le *spamming* facilite la réalisation d'infractions sanctionnées par le droit pénal de l'informatique (§ 3.).

§ 1. LE *SPAMMING*, VÉHICULE D'ESCROQUERIES

384. L'association du *spamming* et du *phishing*. L'emprunt d'identités réelles ou imaginaires sur le réseau constitue un procédé couramment utilisé par les délinquants, soit pour tromper leurs victimes lors de la commission d'une infraction, soit pour orienter les soupçons sur une autre personne et échapper ainsi à tout risque de poursuites. L'association de plus en plus fréquente du *spamming* au *phishing* (« hameçonnage ») illustre clairement cette tendance. Pour rappel, le *phishing* est une « *technique de fraude visant à obtenir des informations confidentielles, telles que des mots de passe ou des numéros de cartes de crédit, au moyen de messages ou de sites usurpant l'identité d'institutions financières ou*

[1080] Le contenu des messages n'étant pas pris en compte dans la définition du *spamming* (sur les éléments constitutifs du *spamming*, v. *supra* : n° 22.

[1081] « *même si* [les] *agissements* [de l'escroc] *sont ingénieux la dimension informatique ne leur confère pas un aspect particulier* » (Pierre-Marie REVERDY, *La matière pénale à l'épreuve des nouvelles technologies*, thèse sous la direction de Corinne Mascala, Toulouse 1, 5 décembre 2005, spéc. n° 141, p. 84 et s.).

d'entreprises commerciales »[1082]. La pratique révèle que ce genre d'attaque se réalise souvent par l'intermédiaire d'envoi massif de *spams* pour accroître son efficacité[1083]. Le processus peut être décrit de la façon suivante : le délinquant utilise l'identité d'une personne morale (institutions financières, organismes publics[1084], entreprises commerciales) afin de créer un climat de confiance et inciter ainsi le destinataire du *spam* à communiquer plus facilement ses données bancaires ou financières (numéros de carte bancaire ou de compte bancaire) ou toute autre donnée nominative (mots de passe, identifiant). Une fois en possession de ces informations, le *phisher* usurpe l'identité de la victime pour lui soustraire de l'argent ou lui dérober d'autres données nominatives. Dans ce cas de figure, nous verrons que le « spammé » pourra engager une action pénale sur le fondement de l'escroquerie. Pour le démontrer, il conviendra de déterminer les éléments constitutifs de l'escroquerie pour ensuite vérifier dans quelles hypothèses le *spamming* pourra être poursuivi au titre de ce délit (A.) et à quelle sanction le « spammeur » risque de s'exposer (B.).

A. LES ELEMENTS CONSTITUTIFS DE L'ESCROQUERIE

385. Élément légal. Aux termes de l'article 313-1 du Code pénal, l'escroquerie est définie comme « *le fait, soit par l'usage d'un faux nom ou d'une fausse qualité, soit par l'abus d'une qualité vraie, soit par l'emploi de manœuvres frauduleuses, de tromper une personne physique ou morale et de la déterminer ainsi, à son préjudice ou au préjudice d'un tiers, à remettre des fonds, des valeurs ou un bien quelconque, à fournir un service ou à consentir un acte opérant obligation ou décharge* ». De façon classique, nous étudierons chacun des éléments constitutifs de cette infraction, à savoir : la condition préalable, c'est-à-dire le bien susceptible d'escroquerie (1.), l'élément matériel (2.) et enfin, l'élément moral (3.).

[1082] Définition de la Commission générale de terminologie et de néologie, J.O. du 12 février 2006, disponible sur : http://franceterme.culture.fr/FranceTerme/recherche.html.
[1083] David PERE et David FOREST, « L'arsenal répressif du phishing », art. préc. : « *le phishing doit être abordé comme un dérivé du spamming* ».
[1084] Par exemple, la Caisse d'Allocations familiales ou l'administration fiscale.

1. Condition préalable : le bien susceptible d'escroquerie

386. L'escroquerie vise soit à remettre des fonds, des valeurs ou un bien quelconque, soit à fournir un service, soit à consentir un acte opérant obligation ou décharge. Envisageons ces trois hypothèses et les conséquences qui en découlent.

387. Des fonds, des valeurs ou un bien quelconque. À l'instar de l'ancienne rédaction du Code pénal, l'escroquerie peut porter sur des fonds. Elle peut désormais porter également sur des « valeurs ». Il convient toutefois de noter qu'il ne s'agit pas d'un réel ajout puisque les fonds et les valeurs « *désignent la même chose* » [1085]. Plus intéressante est l'introduction du terme « bien » dans le Code pénal de 1994 puisqu'elle élargit considérablement le champ de l'incrimination de l'article 313-1 précité. En effet, le bien au sens du droit pénal peut avoir un caractère tant matériel qu'incorporel, pourvu que ce dernier revête une valeur vénale. Le bien quelconque peut donc porter « *sur tout élément exploitable même sans consistance matérielle comme l'obtention d'une information ou même d'une idée quelconque* » [1086]. Cet ajout est donc essentiel pour notre étude puisque les contenus des *spams* sont destinés non seulement à obtenir la remise de numéraire mais également la transmission des coordonnées bancaires du destinataire, données par nature immatérielle, mais dont la valeur économique est indiscutable.

388. L'escroquerie de service. Ce type d'escroquerie constitue l'innovation majeure du Code pénal de 1994 en la matière. Cette nouvelle incrimination permet ainsi de poursuivre et de sanctionner toute personne ayant bénéficié d'un service indu. Tel est le cas, par exemple, lorsque dans le cadre d'un contrat d'affacturage, le client transmet au factor des factures relatives à des livraisons alors que ces dernières n'ont jamais été effectives [1087].

[1085] Michèle-Laure RASSAT, *Droit pénal spécial : Infractions des et contre les personnes*, 5e éd., Dalloz, coll. *Précis*, 2006, spéc. n° 114, p. 140 ; *Escroquerie, J.-Cl. Pénal Code, Art. 313-1 à 313-3*, Fasc. 20, 2009, spéc. n° 35.

[1086] La jurisprudence a ainsi reconnu que l'escroquerie pouvait porter sur un fichier de clientèle, le point de départ d'un scénario, d'un jeu électronique, d'un roman, un « scoop » de presse, (sur ce point, v. Michèle-Laure RASSAT, *Escroquerie*, fasc. préc., 2009, spéc. n° 36.) ; *Droit pénal spécial : Infractions des et contre les personnes*, *ibid.*, spéc. n° 114, p. 140. – V. par ex. TGI Paris, 12e ch. corr., 13 janv. 1982, *D.* 1982, I.R., pp. 501-502, obs. M. Vasseur ; *D.* 1985, I.R., p. 46, obs. J. Huet (en matière de faux ordres de virement : l'escroquerie avait consisté à remettre au service informatique d'une banque une bande magnétique contenant 139 ordres de virement d'un montant de vingt-un millions de francs). – Rappr. TGI Paris, 13e ch. corr., 9 févr. 1982, *D.* 1982, I.R., p. 502, note M. Vasseur. – TGI, 12e ch., 26 juin 1995, *FRANCE TELECOM c/ Dicko*, jugement préc. (utilisation du numéro et du code confidentiel d'un tiers pour établir une communication téléphonique sur le compte de ce dernier constitutive d'escroquerie à l'égard de FRANCE TELECOM et du titulaire de la carte).

[1087] Cass. crim., 19 mars 2008, *inédit*, pourvoi n° 07-86.137 ; *Juris-Data* n° 2008-043756. – V. ég. Cass. crim., 3 juin 1985, pourvoi n° 83-95.073, *Bull. crim.*, n° 211.

389. Acte opérant obligation ou décharge. L'escroquerie peut enfin être constituée lorsque la victime est amenée à signer un acte qui déchargera l'escroc d'une obligation ou qui lui confèrera des droits qu'il n'aurait pas eus [1088].

2. L'élément matériel

390. L'escroquerie est un délit de commission, constitué dès lors qu'il est démontré qu'un acte de tromperie (a.) a déterminé la remise d'un bien quelconque à l'escroc (b.) causant un préjudice à la victime (c.).

a. L'acte de tromperie

391. L'insuffisance du simple mensonge. Par principe, le simple mensonge, qu'il soit écrit ou oral, ne suffit pas à caractériser l'escroquerie, à moins qu'il porte sur le nom ou la qualité de l'agent. Hormis ces deux dernières hypothèses, la chambre criminelle de la Cour de cassation considère que le simple mensonge « *ne peut constituer une manœuvre caractéristique du délit d'escroquerie, s'il ne s'y joint aucun fait extérieur ou acte matériel, aucune mise en scène ou intervention d'un tiers, destinés à donner force et crédit aux allégations mensongères du prévenu* » [1089].

392. Un acte positif. La tromperie peut consister en l'un des actes positifs suivants : l'usage d'un faux nom ou d'une fausse qualité, l'abus d'une qualité vraie ou le recours à une manœuvre frauduleuse. Il convient toutefois de préciser que l'agissement mis

[1088] V. par ex. Cass. crim., 10 déc. 1970, *Ministère Public et Mairie de la ville de Nice c/ Baraldini*, 1re espèce, *JCP* 1972, éd. *G*., II. 17277, note R. Gassin (« [l']*utilisation d'une rondelle sans valeur pour déclencher le mécanisme d'un* […] *« parcmètre » constitue une manœuvre frauduleuse destinée, par le déplacement de l'aiguille, à obtenir décharge du prix du stationnement en persuadant les contrôleurs du paiement de ce prix* ».

[1089] Cass. crim., 11 févr. 1976, pourvoi n° 75-91.806 ; *Bull. crim.*, n° 54, p. 128 ; *D.* 1976, p. 295, note Rapp. Dauvergne. – V. dans le même sens, Cass. crim., 16 oct. 1957, *Bull. crim.* 1957, n° 636 ; *JCP* 1957, éd. G., IV. 166 (jugeant que si les mensonges « *sont accompagnés d'actes extérieurs ou d'une mise en scène destinée à leur donner crédit, de simples mensonges constituent une escroquerie* »). – Toutefois, il convient de préciser que la jurisprudence a tendance à assouplir cette solution et à sanctionner le simple mensonge, v. sur ce point, Michèle-Laure RASSAT, *Droit pénal spécial : Infractions des et contre les personnes*, *op. cit.*, spéc. n° 116, pp. 142-143 ; fasc. préc., spéc. n° 43. – V. ég. Marie-Paule LUCAS DE LEYSSAC pour qui l'escroquerie par manœuvre peut résulter d'un simple mensonge. Sans reconnaître une portée absolue à cette affirmation, celle-ci viendrait restreindre la règle selon laquelle le simple mensonge ne suffit pas à caractériser une escroquerie. L'escroquerie par manœuvre serait ainsi composée de trois degrés : « *1° mensonge renforcé par un élément extérieur emportant manœuvres de type classique ; 2° le mensonge simple non renforcé par un élément extérieur mais constitutif de manœuvres parce que portant sur un point précis sur lequel le droit civil reconnaît une obligation de renseignement fondée sur l'idée de confiance légitime ; 3° le simple mensonge, non situé, insuffisant à constituer la manœuvre parce que couvert par une obligation de vérification ou de contrôle* » (« L'escroquerie par simple mensonge ? », *D.* 1981, chron., p. 17 et s., spéc. p. 24).

en cause ne pourra être sanctionné sur le fondement de l'escroquerie que si l'acte de tromperie a été effectivement utilisé afin de persuader la victime de la véracité d'une information ou d'une situation fausse. Reprenons successivement ces quatre hypothèses pour déterminer comment les juges ont eu l'occasion de les appliquer.

393. L'usage d'un faux nom. Le faux nom s'entend comme le faux nom patronymique ou, en cas de risque de confusion, comme le faux prénom [1090] ou le faux pseudonyme [1091]. Dans tous ces cas de figure, le « faux nom », quelle que soit sa forme, doit nécessairement être celui d'une personne physique. Caractérise ainsi l'usage d'un faux nom le fait de payer des marchandises au moyen de cartes de crédit volées en apposant des signatures apocryphes [1092]. En revanche, la chambre criminelle de la Cour de cassation a jugé que « *l'en-tête " Hôtel du Département " et la référence au " Conseil Général " dans l'adresse où devait être envoyée la facture du faire-part, ne peuvent s'analyser en l'usage d'un faux nom* » [1093].

394. L'usage d'une fausse qualité. La fausse qualité consiste, par exemple, à se prétendre mensongèrement représentant d'un service officiel [1094], conseiller financier [1095], ou encore démarcheur de l'annuaire officiel des PTT [1096], etc.

395. L'abus de qualité vraie. Toute personne dont la fonction inspire une certaine confiance pourra être sanctionnée sur le fondement de l'abus de qualité vraie dès lors que cette qualité est de nature à donner à des allégations mensongères l'apparence de la sincérité et à déterminer la victime à accorder sa confiance. La notion d'abus de qualité vraie a ainsi pu être mise en œuvre à l'encontre d'un notaire [1097], d'un huissier [1098], d'un avocat [1099], d'un

[1090] CA Paris, 16 sept. 1999, *Juris-Data* n° 1999-094960. – Cass. crim. 29 mars 2006, *Juris-Data* n° 2006-033128, *Comm. com. électr.* juill.-août 2006, comm. 117, pp. 39-40, note É. A. Caprioli.
[1091] CA Paris, 1er oct. 2001, *Juris-Data* n° 2001-163093.
[1092] Cass. crim. 19 mai 1987, *Gaz. Pal.* 1988, 1, somm., p. 5.
[1093] Crim. 27 oct. 1999, pourvoi n° 98-86.017 ; *Juris-Data* n° 199-004318, *Bull. crim.*, n° 235.
[1094] Cass. crim., 9 juill. 1982, *inédit.*
[1095] Cass. crim., 16 mars 1987, pourvoi n° 86-92.932 ; *Bull. crim.*, n° 124.
[1096] Cass. crim., 21 juill. 1966, pourvoi n° 66-90.465 ; *Bull. crim.*, n° 208.
[1097] Cass. crim., 11 mars 2009, pourvoi n° 08-83.401 ; *Juris-Data* n° 2009-047746 ; *Dr. pénal* juin 2009, comm. 81, p. 31, note M. Véron (abuse de sa qualité le notaire qui fait signer un compromis de vente subordonné à l'acquisition d'un autre immeuble en sachant que le propriétaire de cet immeuble refuse de la céder au prix indiqué).
[1098] CA Douai, 16 mars 1953, *D.* 1954, somm., p. 3.
[1099] Cass. crim., 30 juin 1999, *Bull. crim.* 1999, n° 170 ; *D.* 1999, I.R., p. 224.

directeur d'une agence d'un établissement bancaire [1100], d'un juriste [1101], d'un directeur comptable d'une entreprise [1102], etc.

396. Le recours à des manœuvres frauduleuses. Il s'agit de l'exercice d'une activité « *destinée à convaincre quelqu'un de faire quelque chose de faux* » [1103]. L'escroc a recours à trois procédés différents qui ont pour finalité de renforcer le mensonge initial et de rendre ce dernier le plus vraisemblable possible. Il peut tout d'abord s'agir d'un écrit, de documents authentiques ou falsifiés. La manœuvre frauduleuse peut également consister en l'intervention d'un tiers, qu'il soit de bonne ou de mauvaise foi, réel ou fictif. Enfin, l'escroquerie peut résulter d'une mise en scène orchestrée par l'escroc destinée à tromper la personne, à la manipuler afin de la persuader de la véracité de la situation chimérique alléguée. Cette dernière hypothèse est celle qui retiendra tout particulièrement notre attention en raison des situations similaires que l'on peut retrouver sur l'internet. Enfin, il convient de préciser que le recours à l'un de ces trois procédés sera pénalement punissable au titre de l'escroquerie si et seulement si les manœuvres frauduleuses sont motivées par la volonté de l'escroc de convaincre la victime d'une situation fausse [1104].

397. Quelques exemples d'escroquerie. La mise en scène peut ainsi consister, par exemple, à se prétendre spécialiste d'un grand peintre et à organiser une exposition de tableaux présentés comme étant des œuvres inédites de l'artiste alors que les expertises ordonnées ont révélé qu'il s'agissait en réalité d'« *œuvres médiocres, malhabiles, primaires et naïves, sans lien possible avec le peintre* » [1105]. Caractérise encore l'existence de manœuvres frauduleuses le fait pour un commerçant d'utiliser un terminal de paiement électronique, remis par une banque et destiné à recevoir les règlements de ses clients, pour effectuer des achats fictifs avec sa carte bancaire personnelle et obtenir ainsi des remises de fonds indues de la part de cet établissement bancaire [1106]. Les manœuvres frauduleuses

[1100] Cass. crim., 1er avr. 1968, pourvoi n° 67-92557 ; *Bull. crim.* 1968, n° 115 ; *JCP* 1968, éd. G., IV. 91.
[1101] Cass. crim., 8 avr. 2010, pourvoi n° 09-83961, *inédit* (usage de la qualité de juriste).
[1102] Cass. crim., 23 mars 1978, pourvoi n° 77-92792 ; *Bull. crim.* 1978, n° 116 ; *D.* 1979, p. 319, note B. Bouloc ; *Rev. sc. crim.* 1979, p. 343 et s., obs. B. Bouzat (condamnation du directeur comptable d'une entreprise industrielle qui, abusant de ses pouvoirs, s'était fait remettre par le banquier de la société la somme de huit millions d'euros, par virement sur le compte bancaire de l'entreprise et à l'insu de son président, dans un but étranger à son mandat).
[1103] Michèle-Laure RASSAT, *Escroquerie*, fasc. préc., spéc., n° 69.
[1104] V. par ex. Cass. crim., 19 juill. 1966 , *JCP* 1966, éd. G., IV. 134 (« *il n'y a manoeuvre frauduleuse* […] *que dans la mesure où est établie l'existence d'une fausse entreprise, apparente ou non, poursuivant ses opérations par des moyens frauduleux et s'efforçant de faire des dupes* »). – Il peut s'agir d'une entreprise totalement fictive. Tel est le cas, par exemple, …. (Cass. crim., 30 janv. 1997, pourvoi n° 96-81270, *Juris-Data* n° 1997-001347).
[1105] CA Rennes, 28 sept. 2000, 3e ch. corr., *Juris-Data* n° 2000-141862, *JCP* 2001, éd. G., II, 10592, note C. T. Geffroy et P. Belloir.
[1106] Cass. crim., 13 sept. 2006, pourvoi n° 05-81.737; *Juris-Data* n° 2006-035236 ; *Bull. crim.*, n° 221, p. 784 ; *Dr. pénal* déc. 2006, comm. 158, note M. Véron ; *JCP* 2007, éd. G., II. 10033, note J. Lasserre-Capdeville ; *RTD com.* 2007, p. 248, obs. B. Bouloc ; *RTD civ.* 2007, p. 350, obs. J. Mestre et B. Fages.

peuvent également consister dans le fait de se faire remettre par des tiers des sommes importantes leur permettant faussement de bénéficier de prestations obtenues grâce à une mise en scène. Il en est ainsi lorsque les candidats ont été attirés par une prétendue loterie organisée dans une résidence hôtelière de luxe, où les lots, apparemment tous gagnants, devaient être retirés [1107]. On peut également mentionner l'escroquerie à la publicité. En effet, même si la publicité trompeuse, devenue pratique commerciale trompeuse, fait l'objet d'une incrimination distincte [1108], la chambre criminelle de la Cour de cassation a jugé que cette pratique pouvait également être sanctionnée sur le fondement de l'escroquerie dans la mesure où il s'agit d'infractions distinctes et donc susceptibles de poursuites sous une double qualification [1109]. Une autre hypothèse est celle de l'escroquerie à la charité. Cette forme d'escroquerie, très ancienne, consiste à demander des fonds en quêtant au profit de personnes mensongèrement handicapées et/ou à vendre des produits supposés être confectionnés par ces derniers et dont les bénéfices de la vente leur reviendraient [1110]. Dans ces hypothèses, les procédés utilisés par l'escroc ne peuvent s'analyser en un simple mensonge. En effet, l'organisation de campagne publicitaire, le nombre et le volume des moyens mis en œuvre sont nature à donner force et crédit à la prétendue entreprise de charité et constituent, à ce titre, une mise en scène destinée à convaincre de l'existence de cette dernière. Constitue encore une escroquerie le fait d'arguer d'une solvabilité mensongère afin de persuader la victime qu'il dispose d'une situation financière de nature à inspirer la confiance et à déterminer la remise du bien convoité [1111] ou de prétendre avoir un droit dont il n'est pas

[1107] Cass. crim., 7 sept. 2005, *inédit*, pourvoi n° 04-87548; *Juris-Data* n° 2005-030008.
[1108] Art. L. 121-1 C. conso. – Sur cette incrimination, v. *infra* : n° 413 et s.
[1109] Cass. crim., 10 mai 1978, pourvoi n° 77-91.445 ; *Bull. crim.*, n° 148 ; *D.* 1978, I.R., p. 348, obs. G. Roujou de Boubée.
[1110] Cass. crim. 25 mars 1968, *D.* 1958, somm., p. 131 (se rend coupable d'escroquerie le gérant d'une société ayant pour objet l'achat et la vente à domicile de produits d'aveugles, qui organise une campagne publicitaire déterminant les acheteurs à verser un prix supérieur à la valeur commerciale des marchandises vendues, dans la croyance que le surplus reviendrait aux aveugles. Or cette société ne produisait rien, n'utilisait pas d'aveugles et se fournissait en savonnettes et en produits d'entretien auprès d'autres sociétés. Les juges ont ainsi jugé que l'exhibition de cartes spéciales délivrées aux courtiers par le gérant ainsi que des emballages à bandes tricolores portant la mention « conditionnée par les aveugles », constituaient une mise en scène à l'égard des clients, donnant à ce commerce une fausse apparence d'intérêt général et philanthropique). – V. ég. Cass. crim., 4 nov. 1969, *D.* 1970, p. 169 (création d'une société anonyme à participation ouvrière dont la raison sociale est « Les aveugles travailleurs de France »). – CA Paris, 9e ch. A, 29 mai 1995, *JurisData* n° 1995-022909 ; *Dr. pénal* nov. 1995, comm. 251, p. 7 et s., obs. M. Véron *; Rev. sc. crim.* avr.-juin 1996, p. 379, obs. R. Ottenhof (prévenus se livrant à une « *publicité intensive* » à l'adresse d'une clientèle aisée pour l'amener à consentir des dons au bénéfice prétendu d'enfants déshérités). – CA Paris, 1er juin 1995, *JurisData* n° 1995-022908, *Rev. sc. crim.* avr.-juin 1996, p. 379, obs. R. Ottenhof (entreprise dont l'objet consistait à démarcher des clients en prétendant que les fonds recueillis étaient destinés aux œuvres de la police).
[1111] V. par ex. Cass. crim., 15 févr. 1961, *D.* 1961, jurispr., p. 276 (« *La remise, pour déterminer un prêt, d'une chose dont l'emprunteur ne pouvait valablement disposer à cet effet et qui était par suite sans valeur, constitue par là même un acte matériel et extérieur ; ayant pour objet, d'autre part, de persuader au prêteur l'existence dans ses mains d'un gage négociable et de faire naître en lui l'espérance chimérique de la réalisation éventuelle de ce gage, ce fait, s'il est accompli de mauvaise foi, constitue une manœuvre frauduleuse dans les termes de l'article* [313-1 du Code pénal] ». – Cass. crim., 21 déc. 1971, *D.* 1972, jurispr., p. 465, note J.-M. Rétant (ont commis une escroquerie au préjudice du Trésor Public les prévenus qui ont utilisé de fausses factures afférentes à des achats fictifs afin de se constituer indûment un crédit de taxes qu'ils ont imputé sur le montant des sommes dont ils étaient redevables). – Cass. crim., 12 sept. 2006, pourvoi n° 05-87.609, *Juris-Data* n° 2006-035232 ; *Dr.*

bénéficiaire en prétextant l'existence d'un crédit imaginaire. Cette hypothèse s'est notamment illustrée dans des cas d'escroquerie à la TVA [1112]. Parmi les très nombreuses formes d'escroquerie, on peut enfin citer celle qui consiste à éveiller chez la victime l'espoir d'un événement chimérique – en particulier des profits importants – dont l'escroc prétend pouvoir éviter ou faciliter sa réalisation [1113].

398. Illustrations de cas d'escroquerie commis *via* le *spamming*. L'usage d'un faux nom ou d'une fausse qualité s'illustre dans de nombreuses hypothèses de *phishing* commis *via* des *spams*. Tel est le cas lorsque l'expéditeur a recours à un envoi massif d'*e-mails*, apparemment authentiques en utilisant l'identité d'un organisme officiel – un établissement bancaire (CIC, Crédit Agricole, Société Générale,…), un FAI (Orange, Free, Alice, …) voire, un service public (Caisse des Allocations Familiales, Administration fiscale) [1114] – et dans lesquels il est demandé aux destinataires, sous un prétexte fallacieux [1115], de mettre à jour leurs données bancaires ou autres informations personnelles, en cliquant sur un lien menant vers un faux site *Web*, copie conforme du site officiel. En jouant sur cette confiance qu'inspire un site Internet connu, l'interlocuteur communiquera de la sorte plus facilement les informations sollicitées sans se méfier. L'escroquerie est également illustrée dans un cas particulier de *phishing* baptisé « arnaque à la nigériane ». Dans cette hypothèse, l'escroc utilise un faux nom et organise une mise en scène s'appuyant sur des événements prétendument alarmants survenus en Afrique afin de persuader la dupe de lui remettre des fonds en échange d'une contrepartie financière [1116]. C'est ainsi que la

pénal déc. 2006, p. 22, note M. Véron (la présentation de fausses factures pour obtenir indûment une garantie constitue une manœuvre frauduleuse et non un simple mensonge écrit).

[1112] Cass. crim., 6 févr. 1969, pourvoi n° 66-91594 ; *Bull. crim.* 1969, n° 65 ; *JCP* 1969, éd. G., II. 16116, note H. Guérin **(**constitue une escoquerie commise au préjudice du Trésor public le fait pour des commerçants de se constituer des crédits irréguliers d'impôts en faisant intervenir, dans leurs transactions normales, des entreprises de façade, insolvables, soit pour facturer, taxes comprises, des marchandises achetées à des tiers sans facture et sans taxe, soit pour produire lors de la revente de fausses attestations d'exportation et obtenir ainsi du Trésor public la remise de sommes indues). – Cass. crim., 10 déc. 1969, pourvoi n° 67-91.046 ; *Bull. crim.* 1969, n° 335.

[1113] Un prévenu s'est ainsi rendu coupable d'escroquerie pour avoir diffusé des annonces dans les journaux qui promettaient des prêts alors qu'il ne possèdait pas les capitaux et n'était le représentant d'aucun organisme capable de faire face aux demandes de prêts. De telles manœuvres frauduleuses lui ont permis de se faire remettre des sommes d'argent en rémunération de services qu'il savait ne pouvoir rendre (Cass. crim. 14 mars 1967, pourvoi n° 66-92.369 ; *Bull. crim.* 1967, n° 102 ; *D.* 1967, somm., p. 50 : la Cour de cassation a relevé que les annonces auxquelles le prévenu avait eu recours ne constituaient pas de simples promesses mensongères mais une véritable organisation de publicité qui était de nature à leur attribuer force et crédit et caractérisant des manoeuvres frauduleuses ayant pour objet de faire naître l'espérance d'un évènement chimérique).

[1114] Pour des exemples illustrés de chacun de ces cas, v. « Alertes *phishing* », disponible sur : http://www.secuser.com/phishing/index.htm.

[1115] Il est fréquemment invoqué la perte des données clients à la suite d'une panne de réseau.

[1116] Sur ce type de délit, v. *supra :* n° 107. – Pour des exemples illustrés, v. Lambert VERJUS, « Le *spamming* en question : Exemples illustrés et conseils pratiques », nov. 2006, spéc. pp. 11-15, disponible sur : http://statbel.fgov.be/fr/binaries/spamming_in_question_fr_tcm326-42567.pdf. – Pour un exemple d'escroquerie à la nigériane, v. TGI Roche-sur-Yon, 24 sept. 2007, *Ministère public c/ Frank A. et al.*, *Comm. com. électr*. déc. 2007, comm. 158, pp. 45-46, note É. A. Caprioli (en l'espèce, les victimes n'avaient pas été contactées par le biais de *spams* mais d'un site Internet de rencontres et l'escroquerie avait été aggravée par la circonstance qu'elle

Cour d'appel de Rennes a condamné des escroqueries en bande organisée commises selon un déroulement strictement identique : les escrocs contactaient les victimes *via* des *e-mails* usurpant des situations sociales importantes et qui faisaient appel à leur compassion ou leur faisaient espérer une importante somme d'argent afin d'amener les destinataires de ces messages à envoyer des mandats en Côte d'Ivoire pour permettre le transfert de fonds provenant d'un héritage vers la France [1117].

b. La remise du bien

399. Formes de la remise. Comme il a été précisé au préalable, l'acte de tromperie doit être à l'origine de la remise. La Cour de cassation a en effet clairement rappelé que « *le délit d'escroquerie n'est établi qu'en présence de manoeuvres antérieures à la remise et ayant été déterminantes de celle-ci* » [1118]. La remise du bien, objet de l'escroquerie, peut se décliner sous diverses formes juridiques selon la consistance du bien considéré : soit par une tradition matérielle lorsqu'il s'agit d'un meuble corporel, soit par l'exécution de la prestation lorsque l'escroquerie porte sur un bien immatériel.

400. Le *spamming* punissable au titre de la tentative d'escroquerie ? Au stade de la réception du *spam*, seules des manœuvres frauduleuses ont été utilisées mais aucune remise n'a encore eu lieu. Cette situation amène donc à déterminer si le « spammeur » pourrait néanmoins être sanctionné au titre de la tentative d'escroquerie. En d'autres termes, il s'agit de savoir si les manœuvres frauduleuses auxquelles il s'est livré peuvent constituer à elles seules le commencement d'exécution qui rendrait ainsi la tentative punissable. En matière d'escroquerie, le seuil du commencement d'exécution sera franchi dès la réalisation des manœuvres frauduleuses, lorsque celles-ci sont clairement destinées à inciter à la remise [1119]. Dans le cas du *phishing via spamming*, les *e-mails* envoyés sont créés de façon à ressembler le plus fidèlement possible à des messages émanant d'organismes légitimes connus afin d'abuser les destinataires et les encourager à révéler des informations confidentielles. En outre, les manœuvres frauduleuses utilisées dans les messages incriminés – faux nom, fausse

avait été commise en bande organisée. Le tribunal a fait preuve d'une particulière sévérité en prononçant deux condamnations, l'une de 5 ans de prison ferme et l'autre de trois ans pour escroquerie réalisée en bande organisée). – T. corr. Strasbourg, 11 déc. 2007, v. le site disponible sur : http://www.01net.com/editorial/367148/prison-ferme-pour-escroquerie-a-la-nigeriane/.

[1117] CA Rennes, 3e ch., 20 nov. 2007, *Ministère public, F., G. /MM. A. B. C. D. E*, disponible sur : http://www.legalis.net/spip.php?page=jurisprudence-decision&id_article=2291.

[1118] Cass. crim., 8 oct. 2003, pourvoi n° 02-80.449. – L'escroquerie diffère en ce sens de l'abus de confiance puisque dans ce second cas, la remise de la chose a été librement consentie.

[1119] Michèle-Laure RASSAT, *Escroquerie*, fasc. préc., spéc. n° 120.

qualité, mise en scène dans l'arnaque à la nigériane – contiennent systématiquement la sollicitation de remise. Au regard de ces éléments, il ne fait aucun doute que le *spamming* véhiculant un contenu trompeur pourra être sanctionné sur le fondement de la tentative d'escroquerie, peu importe qu'il y ait eu remise du bien.

c. Le préjudice

401. Afin que le délit d'escroquerie soit consommé, il faut encore que la remise cause un préjudice à la victime [1120], que celui-ci soit d'ordre moral ou matériel. Les magistrats ont fait preuve d'une grande sévérité en sanctionnant un prévenu qui avait usé de procédés malhonnêtes pour recouvrir une dette alors même que celle-ci était réelle. Ils ont considéré qu'« *il n'importe que cette somme corresponde à une dette effective dès lors que, pour en obtenir la remise, le créancier a usé de moyens dolosifs privant le débiteur de son libre arbitre* » [1121].

3. L'élément moral

402. L'intention frauduleuse. L'escroquerie est à l'évidence une infraction intentionnelle, la simple imprudence étant insuffisante pour constituer l'infraction [1122]. L'élément coupable repose à la fois sur un dol général et un dol spécial. Le dol général réside dans la volonté d'user d'un faux nom, d'une fausse qualité, d'abuser d'une qualité vraie ou de manœuvres frauduleuses. Le dol spécial porte quant à lui sur le procédé utilisé et le but poursuivi. Il suppose que l'escroc utilise l'un des moyens incriminés par les textes aux fins de tromper sa victime et la conduire à la remise du bien convoité. L'élément moral s'apprécie au moment de l'exécution des manœuvres : c'est au moment où le délinquant agit que ce dernier doit avoir conscience du caractère frauduleux de ses agissements, peu importe le mobile de l'auteur [1123]. Dans la plupart des cas, la preuve de l'intention frauduleuse ne pose

[1120] V. par ex. Cass. crim. 27 oct. 1999, arrêt préc. (« *le préjudice est un élément constitutif de l'escroquerie ; qu'en déclarant l'infraction établie sans préciser la nature du préjudice qui résulterait des agissements du prévenu, la cour d'appel n'a pas caractérisé l'infraction en tous ses éléments constitutifs et a privé sa décision de base légale au regard des textes visés au moyen* »).
[1121] Cass. crim., 30 oct. 1996, pourvoi n° 94-86042, *Juris-Data* n° 1996-005202 (ayant approuvé le cour d'appel d'avoir condamné pour escroquerie en jugeant qu' «).
[1122] CA Paris, 26 mai 1982, *Juris-Data* n° 1982-025335 (ont été relaxés des prévenus qui avaient, de bonne foi, usé d'une qualité qu'ils ne possédaient plus pour déterminer une remise).
[1123] Sur le principe de l'indifférence des mobiles, v. Frédéric DESPORTES et Francis LE GUNEHEC, *Droit pénal général, op. cit.*, spéc. n° 477, p. 436. – Xavier PIN, *Droit pénal général*, 3e éd., Dalloz, coll. *Cours*, 2009, spéc. n° 171 et s., p. 146 et s. – Bernard BOULOC, *Droit pénal général, op. cit.*, spéc. n° 258 et s., p. 239 et s.

aucune difficulté et sera déduite du comportement de la personne poursuivie. Dans l'hypothèse de *phishing* par *spamming*, la preuve de cette intention est aisée à rapporter dans la mesure où l'expéditeur a choisi sciemment de recourir à certaines ruses dans les messages envoyés afin de déterminer le destinataire à lui communiquer ses coordonnées bancaires ou à lui transférer directement de l'argent.

B. SANCTIONS

403. Le *quantum* des peines. L'escroquerie est punie à titre principal d'un emprisonnement de cinq ans et de 375.000 euros d'amende [1124]. Outre les peines complémentaires susceptibles d'être prononcées [1125], l'escroquerie est sanctionnée d'une peine de sept ans d'emprisonnement et 750.000 euros d'amende lorsque celle-ci est réalisée dans des circonstances aggravantes [1126]. En revanche, les peines sont portées à dix ans d'emprisonnement et un million d'euros lorsqu'elle est commise en bande organisée [1127]. On ne peut que saluer la sévérité des textes pénaux qui pourrait s'avérer dissuasive pour lutter contre le *phishing* par *spams*.

§ 2. LE *SPAMMING*, VÉHICULE D'INFRACTIONS ISSUES DU DROIT PÉNAL DE LA CONSOMMATION

404. Si l'internet s'est révélé un formidable outil de prospection commerciale, il demeure un support publicitaire comme un autre. Ainsi, toute publicité réalisée par le biais de ce moyen de communication est soumise au respect des règles encadrant la publicité. Comme nous l'avons souligné dès l'introduction générale, le publipostage électronique, procédé de promotion qui permet de toucher un large public à un faible coût [1128] est toutefois susceptible d'abus comme l'illustre le *spamming*. Profitant des avantages de cette technique publicitaire, les « spammeurs » n'hésitent pas à l'utiliser pour vanter des offres alléchantes afin d'inciter les destinataires à consulter leurs messages. Des études récentes rapportent qu'une forte majorité de *spams* fait la promotion de produits « miracles » promettant l'amélioration de la virilité, une perte de poids rapide et sans effort, une lutte efficace contre

[1124] Art. 313-1, al. 2 C. pén.
[1125] Art. 313-7 et s. C. pén.
[1126] Art. 313-2, 1° à 4° C. pén.
[1127] Art. 313-2, dern. al. C. pén.
[1128] V. *supra* : n° 8.

le vieillissement ou encore annonce le gain d'une somme substantielle [1129]. Dans ces différents cas de figure, le droit de la consommation a vocation à intervenir, en particulier le droit pénal de la consommation, pour sanctionner des pratiques de vente et de promotion de produits et de services illicites.

405. L'année 2008 a été pour le droit de la consommation une année riche en innovations. Le législateur a successivement adopté, en l'espace d'un semestre, deux lois successives venant transposer la directive européenne de 2005 sur les pratiques commerciales déloyales [1130] : la loi n° 2008-3 du 3 janvier 2008 pour le développement de la concurrence au service des consommateurs, dite « loi Châtel » [1131], et la loi n° 2008-776 du 4 août 2008 de modernisation de l'économie, désignée sous son acronyme « loi LME » [1132]. Le Code de la consommation a ainsi fait l'objet d'une refonte substantielle [1133] introduisant de nouvelles infractions rassemblées sous le terme de « pratiques commerciales déloyales ».

[1129] MCAFEE, *Rapport sur le paysage des menaces : 2e semestre 2009*, spéc. p. 6, disponible sur : http://www.mcafee.com/us/local_content/reports/6623rpt_avert_threat_0709_fr.pdf.

[1130] Directive n° 2005/29/CE du Parlement européen et du conseil du 11 mai 2005 relative aux pratiques commerciales déloyales des entreprises vis-à-vis des consommateurs dans le marché intérieur et modifiant la directive n° 84/450/CE du Conseil et les directives n° 97/27/CE, 98/27/CE et 2002/65/CE du Parlement européen et du conseil et le règlement (CE) n° 2006/2004 du Parlement européen et du Conseil, J.O.U.E. n° L 149/22 du 11 juin 2005, p. 22 et s. – Sur cette directive, v. not. Jean-Jacques BIOLAY, « La nouvelle directive européenne relative aux pratiques déloyales : défense prioritaire du consommateur et pragmatisme », *Gaz. Pal*. 10 nov. 2005, n° 314, p. 3 et s. – Guy RAYMOND, « Incidences possibles de la transposition de la directive n° 2005/29/CE du 11 mai 2005 sur le droit français de la consommation », *Cont. conc. conso.* janv. 2006, Étude 1, p. 5 et s. – Dominique FENOUILLET, « Une nouvelle directive pour lutter contre les pratiques commerciales déloyales, *RDC* 2005, p. 1059 et s. – Dahmène TOUCHENT, « La protection du consommateur contre les pratiques commerciales déloyales », *LPA* 2 août 2006, n° 153, p. 11 et s. – Pour une étude comparative de la directive et du droit américain en la matière, v. Amandine GARDE et Michaël HARAVON, « Pratiques commerciales déloyales : naissance d'un concept européen, *LPA* 27 juin 2006, n° 127, p. 9 et s.

[1131] Loi n° 2008-3 du 3 janvier 2008 pour le développement de la concurrence au service des consommateurs, dite « loi Chatel », J.O. du 4 janvier 2008, p. 258 et s. – Sur la genèse de cette loi, v. not. Stéphanie FOURNIER, « De la publicité fausse aux pratiques commerciales trompeuses », *Dr. pénal* févr. 2008, Étude 4, p. 13 et s., spéc. n° 2. – Pour une analyse de cette loi, v. Michel CANNARSA, « La réforme des pratiques commerciales déloyales par la loi Chatel : le droit commun à la rencontre du droit de la consommation », *JCP* 2008, éd. G., I. 180. – Agathe LEPAGE, « Un an de droit pénal de la consommation (mars 2007-avril 2008) », *Dr. pénal* mai 2008, chron. 4, p. 15 et s., spéc. n° 18 et s. – Pour un aperçu général des nombreuses réformes issues de la loi n° 2008-3, v. not. Laurent LEVENEUR, « Un peu de concurrence, beaucoup de droit de la consommation – À propos de la loi n° 2008-3 du 3 janvier 2008 », *JCP* 2008, éd. G., actu. 69. – Guy RAYMOND, « Les modifications au droit de la consommation apportées par la loi n° 2008-3 du 3 janvier 2008 pour le développement de la concurrence au service des consommateurs », *Cont. conc. conso.* mars 2008, Étude 3, p. 8 et s., spéc. n° 15 et s. ; *Actualité : Présentation de la loi n° 2008-3 du 3 janvier 2008 pour le développement de la concurrence au service des consommateurs*, *J.-Cl. Conc.-Conso.*, Fasc. 10, spéc. n° 43 et s.

[1132] Loi n° 2008-776 du 4 août 2008 de modernisation de l'économie, dite « loi LME », J.O. du 5 août 2008, p. 12471 et s. – Pour une étude de cette loi, v. not. Coralie AMBROISE-CASTEROT, « Les nouvelles pratiques commerciales déloyales après la loi LME du 4 août 2008 », *AJ pénal* 2009, p. 22 et s. – Muriel CHAGNY, « Une (r)évolution du droit français de la concurrence ? – À propos de la loi LME du 4 août 2008 », *JCP* 2008, éd. G., I. 196. – Emmanuel DREYER, « Un an de droit de la publicité », *Comm. com. électr*. juill.-août 2008, étude 7, p. 15 et s. – Dominique FENOUILLET, « La loi de modernisation de l'économie du 4 août 2008 et réforme du droit des pratiques commerciales déloyales », *RDC* 2009, p. 128 et s. – Xavier LAGARDE, « Observations sur le volet consommation de la loi de modernisation de l'économie », *LPA* 23 févr. 2009, n° 38, p. 3 et s. – Jérôme LASSERRE CAPDEVILLE, « La substitution du délit de pratiques commerciales trompeuses au délit de publicité fausse ou de nature à induire en erreur », *LPA* 21 nov. 2008, n° 234, p. 8 et s.

[1133] Titre II du livre Ier C. conso.

L'article L. 120-1 du Code de la consommation, créé par la loi Chatel [1134], pose un principe général d'interdiction de ce type de pratique : est considérée comme déloyale, toute pratique « *contraire aux exigences de la diligence professionnelle et* [qui] *altère, ou est susceptible d'altérer de manière substantielle, le comportement économique du consommateur normalement informé et raisonnablement attentif et avisé, à l'égard d'un bien ou d'un service* » [1135]. Entrent ainsi dans le champ d'application de cette disposition, les pratiques commerciales trompeuses, désignées auparavant sous l'appellation de « publicité trompeuse » [1136] et les pratiques commerciales agressives [1137]. À contre-courant d'une tendance générale à la dépénalisation du droit des affaires [1138], ces pratiques sont lourdement sanctionnées [1139] afin de renforcer l'obligation de loyauté [1140] imposée au professionnel. Il convient donc de déterminer dans quelles hypothèses le *spamming* peut être sanctionné d'une part, au titre des pratiques commerciales trompeuses (B.) et d'autre part, sur le fondement des pratiques commerciales agressives (C.) [1141]. Avant cela, nous nous intéresserons à définir la notion de « pratique commerciale », élément matériel commun à ces deux infractions (A.).

[1134] Art. 39 loi n° 2008-3.

[1135] V. Guy RAYMOND, « Les modifications au droit de la consommation apportées par la loi n° 2008-3 du 3 janvier 2008 pour le développement de la concurrence au service des consommateurs », étude préc., spéc. n^{os} 21-22.

[1136] Historiquement, la loi de finances n° 63-628 du 2 juillet 1963 rectificative pour 1963 portant maintien de la stabilité économique et financière (J.O. du 3 juillet 1963, p. 5915 et s.) avait créé l'infraction de publicité mensongère. Celle-ci fut, transformée dix ans plus tard en délit de « publicité fausse ou de nature à induire en erreur », communément désignée par la doctrine sous par la formule plus concise de « publicité trompeuse » et codifiée à l'article L. 121-1 et suivants du Code de la consommation (loi n° 73-1193 du 27 décembre 1973, d'orientation, du commerce et de l'artisanat, dite « loi Royer », J.O. du 30 décembre 1973, p. 14139 et s.). Par la suite, la loi du 3 janvier 2008 a transformé cette infraction en pratiques commerciales trompeuses et a, en même temps, modifié de façon substantielle l'ancienne version de l'article L. 121-1 précité.

[1137] Art. L. 120-1-II C. conso : « *Constituent en particulier des pratiques commerciales déloyales les pratiques commerciales trompeuses définies aux articles L. 121-1 et L. 121-1-1 et les pratiques commerciales agressives définies aux articles L. 121-1 et L. 121-1-1* » (art. 83 loi n° 2008-776).

[1138] Jean-Marie COULON, *La dépénalisation de la vie des affaires*, Doc. fr., coll. *Rapports officiels*, 2008. – Pour un aperçu général de cette question, v. not. Marie-Christine SORDINO, « Flux et reflux du droit pénal au sein du droit des affaires (À propos de la « dépénalisation de la vie des affaires ») », *Gaz. Pal.* 24 mai 2008, n° 145, p. 2 et s. – Kami HAERI, « Réflexions sur le rapport du groupe de travail sur la dépénalisation de la vie des affaires : et le droit pénal n'appartient plus jamais au justiciable », *in* « Dépénalisation de la vie des affaires », Dossier spécial, *Dr. pénal* mars 2008, p. 13 et s.

[1139] Philippe GUILLERMIN, « Droit de la consommation : l'absence d'une véritable alternative à la voie pénale » *in* Dossier : « Quelle dépénalisation pour le droit des affaires », *AJ Pénal* 2008, n° 2, p. 73. – Sur les liens entre la loi n° 2008-3 du 3 janvier 2008 et le droit pénal, v. Agathe LEPAGE, « Un an de droit pénal de la consommation (mars 2007-avril 2008) », chron. préc., spéc. n° 19 et s.

[1140] Rappr. de l'article 1134 du Code civil alinéa 3 relatif à la bonne foi en matière contractuelle. – Sur ce point, v. Dahmène TOUCHENT, « La protection du consommateur contre les pratiques commerciales déloyales », chron. préc.

[1141] Il existe également des sanctions civiles que l'on ne manquera pas d'évoquer. Toutefois, l'objectif étant de trouver des sanctions dissuasives pour tenter de stopper les activités des « spammeurs », le volet pénal retiendra donc tout particulièrement notre attention.

A. LA NOTION DE PRATIQUE COMMERCIALE ET SES IMPLICATIONS

406. Extension du champ de l'incrimination au regard de la nature de l'acte. Bien que la notion de « pratique commerciale » occupe une place centrale dans le Code de la consommation [1142], de façon surprenante, la loi ne l'a pas définie. Or, si la publicité est une notion relativement claire qui renvoie à une communication au public d'un message incitatif, la pratique commerciale qui ne se rapporte qu'à des procédés en rapport avec le commerce aurait, pour sa part, nécessité certaines précisions [1143]. Cette carence est critiquable car elle met à mal le principe de légalité, principe fondamental en matière pénale [1144] dont découle le principe d'interprétation stricte de la norme pénale [1145]. Pour saisir le sens de cette expression, il convient donc d'interroger la directive européenne n° 2005/29/CE du 11 mai 2005. Aux termes de son article 2 d), celle-ci est définie comme : « *toute action, omission, conduite, démarche ou communication commerciale, y compris la publicité et le marketing, de la part d'un professionnel, en relation directe avec la promotion, la vente ou la fourniture d'un produit aux consommateurs* » [1146]. Selon la directive de 2005, trois critères objectifs permettent d'identifier une pratique commerciale, à savoir : son support, l'objet et la nature du contrat conclu et la finalité de cette pratique.

407. Indifférence quant au support. Concernant tout d'abord le support de la pratique, cette précision était clairement contenue dans l'ancien texte français qui visait toute publicité « *sous quelque forme que ce soit* » [1147]. La directive de 2005, moins explicite, semblait néanmoins plaider en ce sens en visant « *toute action, omission, conduite, démarche ou communication commerciale, y compris la publicité et le marketing* » [1148]. Par la référence à la notion de « pratiques commerciales » plutôt qu'à celle de « publicité » issue de l'ancienne rédaction, la loi de janvier 2008 étend ainsi le champ de cette incrimination et permet d'assurer une protection pénale plus étendue des consommateurs contre les pratiques

[1142] Cette notion est l'intitulé du Titre II du Code de la consommation qui couvre les articles L. 120-1 et suivants du même code.
[1143] Sur ce point, v. Stéphanie FOURNIER, « De la publicité fausse aux pratiques commerciales trompeuses », étude préc., spéc. n° 6.
[1144] Art. 111-2 et 111-3 C. pén.
[1145] Art. 111-4 C. pén.
[1146] Art. 2, d) dir. n° 2005/29/CE.
[1147] Ancienne version de l'article L. 121-1 C. conso. – Pour des exemples jurisprudentiels, v. Stéphanie FOURNIER, « De la publicité fausse aux pratiques commerciales trompeuses », étude préc., spéc. n° 7 : certains juges ont considéré que l'infraction de publicité trompeuse pouvait être retenue en raison d'informations figurant sur un emballage de produit, un bon de commande, une facture…).
[1148] Art. 2, d) dir. n° 2005/29/CE.

commerciales déloyales [1149]. Sont ainsi visés tous les modes de communication qu'ils soient de nature orale, écrite, y compris graphique (image, dessin ou photographie), de même que tous les moyens de transmission (presse écrite, radio, télévision, cinéma, téléphone, Internet, courrier postal ou électronique, etc.) [1150].

408. Indifférence quant à l'objet du contrat. À la lecture de la directive n° 2005/29/CE, l'objet de la pratique commerciale apparaît très large puisqu'il englobe « *la promotion, la vente ou la fourniture d'un produit aux consommateurs* » [1151]. Seul importe donc le fait que l'auteur de la pratique incriminée offre « un produit » sur le marché [1152]. La directive de 2005 définit le terme « *produit* » de façon très large comme désignant « *tout bien ou service, y compris les biens immobiliers, les droits et les obligations* » [1153]. S'agissant tout d'abord des biens visés, elle ne fait aucune distinction selon leur nature, celle-ci pouvant être mobilière ou immobilière, comme l'avait déjà reconnu la jurisprudence antérieure à la réforme de 2008 [1154]. Quant au service concerné, il doit également être entendu de façon très large puisqu'il a, par exemple, été jugé que les pratiques commerciales pouvaient concerner des activités relevant de la voyance ou plus largement des sciences occultes [1155]. Enfin, sont également inclus dans cette notion de produits « *les droits et obligations* ». La jurisprudence antérieure à la réforme en offre quelques exemples : des opérations de vente de fonds de commerce [1156] ou celles ayant pour objet la vente de produits financiers [1157] ont été jugées comme entrant dans le champ de l'incrimination de publicité de nature à induire en erreur.

[1149] Guy RAYMOND, « Les modifications au droit de la consommation apportées par la loi n° 2008-3 du 3 janvier 2008 pour le développement de la concurrence au service des consommateurs », étude préc., spéc. n° 25 (« *la publicité* [n'est plus] *que l'un des supports qui peut donner lieu à application de la nouvelle infraction* »).

[1150] Sur cette indifférence du support et pour des illustrations jurisprudentielles, v. Stéphanie FOURNIER, *Pratiques commerciales trompeuses*, *J.-Cl. Lois pénales spéciales*, Fasc. 20, 2008, spéc. n° 13. – Nicolas ÉRESEO, *Pratiques commerciales trompeuses*, fasc. préc., spéc. n^{os} 14 et 15.

[1151] Art. 2, d) dir. n° 2005/29/CE.

[1152] Avant la réforme de 2008, il avait déjà été jugé qu'une personne ne proposant aucun produit ou service ne pouvait être poursuivie au titre de la publicité de nature à induire en erreur (v. en ce sens, à propos d'une association distribuant des tracts devant un palais de justice incitant les passants à agir en justice : Cass. Ass. plén., 8 juill. 2005, pourvoi n° 97-83.023 ; *JurisData* n° 2005-029430 ; *Bull. crim.*, n° 2, p. 10 *; JCP* 2005, éd. G., IV. 2999).

[1153] Art. 2, c) dir. n° 2005/29/CE.

[1154] Avaient ainsi été jugés comme entrant dans le champ d'application de l'ancien article L. 121-1 du Code de la consommation des opérations de vente (v. par ex. Cass. crim., 16 févr. 1982, pourvoi n° 81-92.263 ; *Bull. crim.* 1982, n° 54) ou de location (v. Cass. crim., 28 nov. 2000, pourvoi n° 99-87.262).

[1155] CA Pau, ch. corr., 3 avr. 2008, *Juris-Data* n° 2008-369964 ; *JCP* 2008, éd. G., IV. 2871 (les juges soulignant que le caractère irrationnel de l'activité – en l'espèce, un marabout – et des annonces diffusées dans lesquelles le prévenu garantissait des résultats efficaces et rapides, n'est pas un obstacle à l'application de l'article L. 121-1 du Code de la consommation ; le caractère mensonger n'en étant pas moins avéré. Caractérise ainsi une escroquerie la publication d'une annonce destinée à tromper le lecteur en lui faisant croire en la certitude d'un résultat, en réalité, chimérique ou aléatoire alors qu'il est établi que le travail est inefficace).

[1156] CA Aix-en-Provence, 6 déc. 2006, *Juris-Data* n° 2006-325519.

[1157] Cass. crim., 16 oct. 2007, pourvoi n° 06-88015, *JurisData* n° 2007-041527.

409. Indifférence quant à la nature du contrat. Le terme « fourniture » doit être lui-même entendu largement comme en atteste la référence aux services. De façon générale, il couvre tout contrat à titre onéreux, à savoir : le contrat de louage d'ouvrage, le mandat, le prêt ou le dépôt. Se pose alors la question du sort des contrats à titre gratuit : sont-ils également inclus dans le champ des pratiques commerciales ? La jurisprudence antérieure à la réforme y était favorable : « [l]*es contrats à titre gratuit* […] *entrent dans le champ de la publicité trompeuse* » [1158]. Cette solution semble devoir encore être admise aujourd'hui dans la mesure où il est fréquent qu'une entreprise fasse la promotion de ses biens ou de ses services par le biais d'opérations gratuites telles que des concours, des loteries ou des jeux [1159]. L'article L. 121-1-1, 18° du Code de la consommation plaide d'ailleurs en ce sens puisque selon cette disposition, est réputée trompeuse la pratique qui consiste à « *affirmer, dans le cadre d'une pratique commerciale, qu'un concours est organisé ou qu'un prix peut être gagné sans attribuer les prix décrits ou un équivalent raisonnable* » [1160]. Il convient de conclure que le caractère gratuit de l'opération organisée est indifférent : tout contrat, quelle que soit sa nature, est susceptible d'être sanctionné au titre des pratiques commerciales déloyales.

410. Finalité promotionnelle de la pratique. Pour définir le caractère déloyal d'une pratique, l'article L. 120-1 du Code de la consommation s'attache avant tout à un effet : celui d'altérer « *de manière substantielle le comportement économique du consommateur* » [1161]. Or, cette altération ne peut exister que si cette pratique a un caractère incitatif [1162]. La directive n° 2005/29/CE confirme cette analyse en subordonnant le caractère commercial d'une pratique au fait que celle-ci soit « *en relation directe avec la promotion, la vente ou la fourniture d'un produit aux consommateurs* » [1163]. Le caractère direct révèle que la directive ne couvre que les pratiques qui seraient liées à un contrat conclu ou destiné à être conclu. Toutefois, l'article 3.1. de cette directive sème le trouble en visant les pratiques commerciales déloyales « *avant, pendant* [mais aussi] *après une transaction commerciale portant sur un produit* » alors que le caractère incitatif semble *a priori* inexistant pour les

[1158] Cass. crim., 8 mars 1990, *Juris-Data* n° 1990-001311 ; *JCP* 1990, éd. G., II. 21542, note J.-H. Robert.
[1159] V. en ce sens, Nicolas ÉRESEO, *Pratiques commerciales trompeuses*, fasc. préc., spéc. n° 18.
[1160] V. antérieurement à la réforme de 2008, CA Douai, 14 juin 2005, *Juris-Data* n° 2005-278037 (à propos d'un courrier publicitaire signalant le gain d'un four alors qu'il ne s'agissait en réalité que d'une paire de poêles de faible valeur).
[1161] Art. L. 120-1 C. conso.
[1162] Nicolas ÉRESEO, *Pratiques commerciales trompeuses*, fasc. préc., spéc. n° 20. – V. également en ce sens la directive de 2005 dispose qu'une pratique n'est commerciale que si elle est « *en relation directe avec la promotion, la vente ou la fourniture d'un produit aux consommateurs* » (Art. 2, d) dir. n° 2005/29/CE). Cela rejoint la définition proposée par Philippe CONTE qui préconise que l'on prenne cette « *expression dans son acception la plus banale, celle d'une manière d'exercer une activité commerciale, à travers, notamment, la publicité, les procédures de négociation, les techniques de vente, etc.* » (« Brèves observations à propos de l'incrimination des pratiques commerciales agressives », *Dr. pénal* févr. 2008, Étude 3, p. 7 et s., spéc. n° 6).
[1163] Art. 2 d) dir. 2005/29/CE.

pratiques consécutives à la conclusion d'un contrat. Il convient toutefois de préciser que, même dans ce cas de figure, l'exigence d'incitation pourrait être se vérifier dès lors que la pratique a pour but de poursuivre ou de renouveler une relation commerciale [1164]. L'ajout des hypothèses postérieures à la conclusion d'un contrat est important puisqu'elle permet d'étendre le champ de l'incrimination qui pourrait venir sanctionner des pratiques qui ne pouvaient l'être lorsque la loi visait la seule publicité [1165].

411. En définitive, il apparaît que la pratique commerciale est très largement définie comme toute opération, quels que soient son support et la nature du contrat conclu, ayant pour finalité la promotion de tout bien ou de tout service ou la poursuite ou le renouvellement d'une relation commerciale antérieure. Ainsi, dans tous les cas où le *spamming* a une finalité commerciale, il pourra sans difficulté être qualifié de pratique commerciale au sens du droit de la consommation et le cas échéant, être sanctionné lorsqu'il est déloyal.

412. Restriction du champ de l'incrimination eu égard à l'auteur et à la victime. Si la réforme de 2008 a permis une extension du champ des agissements sanctionnables, elle en a au contraire restreint les contours s'agissant de leur(s) auteur(s). En effet, avant la réforme, le simple particulier qui diffusait une publicité trompeuse pouvait être poursuivi [1166]. Désormais, seuls les professionnels, auteurs de la pratique incriminée, peuvent être poursuivis sur ce fondement. Cette limitation se déduit des références de l'article L. 120-1 du Code de la consommation aux termes de « *pratiques commerciales* », associés au non-respect de la « *diligence professionnelle* ». De même, la directive de 2005 confirme cette analyse en définissant cet auteur comme « *toute personne physique ou morale qui, pour les pratiques commerciales relevant de la présente directive, agit à des fins qui entrent dans le cadre de son activité commerciale, industrielle, artisanale ou libérale, et toute personne agissant au nom ou pour le compte d'un professionnel* » [1167]. Notons enfin que la loi du 3 janvier 2008 est venue apporter une précision concernant l'auteur des pratiques commerciales trompeuses. Avant la réforme, l'article L. 121-5 du Code de la consommation, qui visait « *l'annonceur* », avait conduit la jurisprudence à s'interroger sur le point de savoir si ce dernier devait être entendu comme la personne qui utilisait le message publicitaire pour proposer de contracter ou celle qui avait l'initiative de la diffusion mais qui agissait

[1164] Sur cette possible extension du champ de l'incrimination, v. Stéphanie FOURNIER, « De la publicité fausse aux pratiques commerciales trompeuses », étude préc., spéc. n° 7.
[1165] En effet, l'objet de la publicité étant, par définition, celui de promouvoir un produit ou un service afin d'inciter les consommateurs à se procurer ce bien ou à utiliser ce service, seules étaient visées des pratiques entrant dans le cadre d'un contrat.
[1166] Pour des exemples, v. Nicolas ÉRESEO, *Pratiques commerciales trompeuses*, fasc. préc. , spéc. n° 21.
[1167] Art. 2, b dir. 2005/29/CE.

éventuellement pour le compte d'un tiers. Désormais, le doute est dissipé : seule « *la personne pour le compte de laquelle la pratique commerciale trompeuse est mise en œuvre est responsable, à titre principal, de l'infraction commise* » [1168]. S'agissant enfin de la victime, une nouvelle distinction est créée selon la tromperie en cause [1169] : les tromperies par action sont répréhensibles, qu'elles soient dirigées contre un professionnel [1170] ou contre un profane, en revanche, seules les tromperies par omission s'adressant aux particuliers seront sanctionnées [1171].

B. LE *SPAMMING* AU SERVICE DES PRATIQUES COMMERCIALES TROMPEUSES

413. La preuve du caractère trompeur. Avant de débuter cette étude, il convient de préciser que la loi du 4 août 2008 a créé l'article L. 121-1-1 du Code de la consommation qui définit certaines pratiques commerciales réputées trompeuses. Pour tous les autres cas non visés par ce texte, la preuve du caractère trompeur devra être rapportée par référence au consommateur moyen, défini comme un « *consommateur normalement informé et raisonnablement attentif et avisé* » [1172]. L'article L. 120-1 du Code de la consommation précise en effet qu'un comportement est déloyal dès lors qu'il « *altère ou est susceptible d'altérer le comportement économique* » de ce consommateur de référence. La nouvelle rédaction de l'article L. 120-1 précité élargit ainsi le champ de l'incrimination, la pratique commerciale en cause peut désormais être poursuivie et sanctionnée sans que le consommateur ait été effectivement trompé [1173].

[1168] Sur cette possible extension du champ de l'incrimination, v. Stéphanie FOURNIER, « De la publicité fausse aux pratiques commerciales trompeuses », étude préc., spéc. n° 8.

[1169] Sur la distinction entre les différents cas de tromperie, v. *infra* : n° 415 et s. et n° 420.

[1170] « *Le I* [relatif aux tromperies par action] *est applicable aux pratiques qui visent les professionnels* » (art. L. 121-1, III. C. conso).

[1171] Selon une lecture *a contrario* de l'article L. 121-1, III. C. conso.

[1172] Art. L. 120-1 C. conso. – Sur cette notion de consommateur avisé, v. Agathe LEPAGE, « Un an de droit pénal de la consommation (avril 2008-avril 2009) », *Dr. pénal* mai 2009, chron. 5, p. 15 et s., spéc. n^{os} 24-25. – La notion de « *consommateur normalement informé et raisonnablement attentif et avisé* » était déjà utilisée en matière de publicité trompeuse (v. en ce sens, CA Aix-en-Provence, 14 janv. 1998, *Juris-Data* n° 1998-041496 : la cour d'appel a jugé que « *même si le style employé dans la publicité se voulait volontairement racoleur et tapageur pour attirer l'attention du lecteur, le consommateur moyen n'a pu à la lecture attentive du document être trompé ou induit en erreur sur le contenu de l'offre et a envoyé sa demande en connaissance de cause* »). – En revanche, constituait une publicité de nature à induire en erreur le « consommateur moyen », un message publicitaire annonçant une liquidation totale à des prix sacrifiés et concluant par une mention « tout doit disparaître », puisque ce type de consommateur pouvait s'attendre à trouver des réductions de prix sur l'ensemble des articles en vente et non sur une partie d'entre eux (CA Caen, 6 mars 1998, *Juris-Data* n° 040489). – V. ég. Cass. Crim. 18 déc. 1996, *Rev. sc. crim.* 1998, p. 120, comm. A. Giudicelli. – Pour une référence au « *consommateur d'une intelligence moyenne* », v. not. CA Paris, 13^{e} ch. 16 mai 2008, *Juris-Data* n° 2008-364022.

[1173] Pour des précisions sur l'appréciation de l'élément trompeur, v. Nicolas ÉRESEO qui énonce notamment que « [l]*'appréciation de l'effet trompeur d'une pratique obéit à deux règles qui peuvent être résumées très*

414. Le caractère trompeur redéfini et précisé. À l'instar de la directive de 2005 [1174], la loi du 3 janvier 2008 est venue modifier le texte antérieur [1175] en classant en deux catégories distinctes les pratiques commerciales trompeuses : celles par action (1.) et celles par omission (2.). Après avoir examiné successivement ces deux types de pratiques, nous nous attacherons à définir leur élément moral (3.) pour envisager enfin les sanctions encourues et les poursuites auxquelles pourrait s'exposer le délinquant (4.).

1. Les tromperies par action

415. Parmi les tromperies par action, on dénombre notamment trois sous-catégories, à savoir : les pratiques créant une confusion entre deux biens ou deux signes concurrents (a.) [1176] et les allégations fausses ou de nature à induire en erreur (b.) et enfin celle de nature à faire naître une incertitude quant à l'annonceur (c.). À ce dispositif, la loi du 4 août 2008 est venue préciser dans chaque catégorie, les cas dans lesquels la pratique commerciale est réputée trompeuse afin de renforcer la sécurité juridique [1177]. Nous n'évoquerons ici que les dispositions susceptibles d'intéresser spécifiquement notre étude que nous illustrerons grâce à des exemples issus des diverses pratiques auxquelles ont recours les « spammeurs ».

a. La confusion

416. Définition et applications au *spamming*. L'article L. 121-1, I, 1° du Code de la consommation énonce qu'une pratique commerciale est trompeuse « [l]*orsqu'elle crée une confusion avec un autre bien ou service, une marque, un nom commercial, ou un autre signe d'distinctif d'un concurrent* ». Cette hypothèse implique donc que le « spammeur » soit un concurrent de la victime. Il convient de souligner que ce cas a peu de risque de se rencontrer en ce sens où le professionnel qui agirait de la sorte nuirait gravement à sa réputation et à son image. En revanche, un cas plus intéressant pour notre étude est celui visé par l'article L.

simplement : tout ce qui est trompeur n'est pas faux et tout ce qui est faux n'est pas trompeur » (fasc. préc., spéc. n[os] 54-57)). – Pour des illustrations récentes de l'appréciation du caractère trompeur, v. Agathe LEPAGE, « Un an de droit pénal de la consommation (avril 2009-avril 2010) », *Dr. pénal* mai 2010, chron. 4, p. 23 et s., spéc. n[os] 27-31, p. 28 et s.

[1174] Art. 6 et 7 dir. 2005/29/CE.

[1175] Avant la réforme de 2008, la publicité était considérée comme trompeuse par la seule circonstance qu'elle contienne « *sous quelque forme que ce soit, des allégations, indications ou prestations fausses ou de nature à induire en erreur* ».

[1176] Art. L. 121-1, I, 1° C. conso.

[1177] Art. L. 121-1-1 C. conso.

121-1, I, 13° du Code la consommation. Selon cette disposition, est réputée trompeuse la pratique qui a pour objet « *de promouvoir un produit ou un service similaire à celui d'un autre fournisseur clairement identifié, de manière à inciter délibérément le consommateur à penser que le produit ou le service provient de ce fournisseur alors que tel n'est pas le cas* » [1178]. Cette hypothèse pourra s'illustrer en matière de *spamming* chaque fois que les messages dont le contenu propose, par exemple, la vente de produits de luxe à bas prix alors qu'il ne s'agit que de vulgaires contrefaçons ou encore celle de logiciels prétendument officiels et qui ne sont en réalité que des exemplaires piratés [1179].

b. Les allégations fausses ou de nature à induire en erreur

417. Champ d'application et applications au *spamming*. L'article L. 121-1, I, 2° du Code de la consommation considère comme trompeuse toute pratique commerciale qui « *repose sur des allégations, indications ou présentations fausses ou de nature à induire en erreur* » [1180]. La tromperie peut porter sur divers éléments [1181] tels que : l'existence, la disponibilité, la nature du bien ou du service [1182] ou encore sur ses caractéristiques essentielles [1183]. Ce dernier grief apparaît de loin le plus souvent soulevé dans la mesure où il couvre la plupart des éléments pouvant déterminer le consommateur à choisir tel produit ou

[1178] Art. L. 121-1-1, 13° C. conso.

[1179] Pour des exemples illustrés, v. Lambert VERJUS, « Le *spamming* en question : Exemples illustrés et conseils pratiques », préc., spéc. pp. 27-28..

[1180] Art. L. 121-1, I, 2° C. conso. – Cette disposition est sensiblement similaire à l'ancienne version de l'article L. 121-1 du Code de la consommation relatif à la publicité trompeuse qui sanctionnait les pratiques commerciales trompeuses (publicité trompeuse, selon la lettre de l'époque) qui contenaient « *sous quelque forme que ce soit, des allégations, indications ou prestations fausses ou de nature à induire en erreur* » et qui étaient, *a fortiori*, des tromperies par action.

[1181] Pour une étude très détaillée et de nombreux exemples jurisprudentiels illustrant chacun des éléments sur lesquels peut porter la tromperie, v. Nicolas ÉRESEO, *Pratiques commerciales trompeuses*, fasc. préc., spéc. n° 31 et s.

[1182] À ce titre, le Code de la consommation répute trompeur le fait de « *proposer l'achat de produits ou la fourniture de services à un prix indiqué sans révéler les raisons plausibles que pourrait avoir le professionnel de penser qu'il ne pourra fournir lui-même, ou faire fournir par un autre professionnel, les produits ou services en question ou des produits ou services équivalents au prix indiqué, pendant une période et dans des quantités qui soient raisonnables compte tenu du produit ou du service, de l'ampleur de la publicité faite pour le produit ou le service et du prix proposé* » (art. L. 121-1-1, 5° C. conso.) ou le fait « *de proposer l'achat de produits ou la fourniture de services à un prix indiqué, et ensuite : a. De refuser de présenter aux consommateurs l'article ayant fait l'objet de la publicité ; b. Ou de refuser de prendre des commandes concernant ces produits ou ces services ou de les livrer ou de les fournir dans un délai raisonnable ; c. Ou d'en présenter un échantillon défectueux, dans le but de faire la promotion d'un produit ou d'un service différent* » (art. L. 121-1-1, 6° C. conso.) ou encore celui qui consiste à « *déclarer faussement qu'un produit ou un service ne sera disponible que pendant une période très limitée ou qu'il ne sera disponible que sous des conditions particulières pendant une période très limitée afin d'obtenir une décision immédiate et priver les consommateurs d'une possibilité ou d'un délai suffisant pour opérer un choix en connaissance de cause* » (art. L. 121-1-1, 7° C. conso.). – Enfin, l'article L. 121-1-1, 17° du même Code répute trompeuse la pratique qui a pour objet « *de communiquer des informations matériellement inexactes sur les conditions de marché ou sur les possibilités de trouver un produit ou un service, dans le but d'inciter le consommateur à acquérir celui-ci à des conditions moins favorables que les conditions normales de marché* ».

[1183] Art. L. 121-1, I, 2 b) C. conso.

tel service plutôt que tel autre. Au titre des caractéristiques essentielles, on peut citer notamment [1184] : les qualités substantielles [1185], la composition [1186], l'origine, la quantité, les conditions de son utilisation et son aptitude à l'usage, ses propriétés et les résultats attendus de son utilisation [1187]. Il convient de préciser en outre que le Code de la consommation répute trompeur le fait « *d'affirmer* […] *qu'un concours est organisé ou qu'un prix peut être gagné sans attribuer les prix décrits ou un équivalent raisonnable* » [1188], le fait « *d'affirmer d'un produit ou d'un service qu'il augmente les chances de gagner aux jeux de hasard* » [1189] ou encore « *d'affirmer faussement qu'un produit ou une prestation de services est de nature à guérir des maladies, des dysfonctionnements ou des malformations* » [1190]. On remarque que ces présomptions épousent parfaitement de nombreuses hypothèses de *spamming* telles que la promotion de prétendues loteries nationales [1191] ou encore la vente de cures « miracles » qui promettent un amaigrissement rapide [1192], de meilleures performances sexuelles ou une lutte efficace contre la calvitie. Enfin, la tromperie peut encore porter sur « *l'identité, les qualités, les aptitudes et les droits du professionnel* » [1193] et qui aurait pour effet de permettre à son auteur de prétendre disposer à tort d'un titre, d'un diplôme ou d'une qualification [1194].

[1184] Art. L. 121-1, I, 2°, b) C. conso. – V. Agathe LEPAGE, « Un an de droit pénal de la consommation (avril 2008-avril 2009) », chron. préc., spéc. n[os] 22-23. – Nous n'évoquerons que les dispositions susceptibles d'intéresser notre étude.

[1185] Rappr. de l'article 1110 C. civil. – V. par ex. CA Paris, 13[e] ch., 5 mai 2008, *Juris-Data* n° 2008-362810 (caractérise la publicité trompeuse une étiquette collée sur la pochette d'un disque et portant la mention « Édition limitée, CD bonus 6 titres acoustiques » dans la mesure où elle fait croire que le disque contient des morceaux non commercialisés alors qu'en réalité le disque n'est qu'une compilation d'anciens titres).

[1186] V. par ex. CA Paris, 31 janv. 2007, *JurisData* n° 2007-340182 (a été jugée trompeuse la mention indiquant « *équivalent d'un yaourt aux fruits* » pour des produits simplement aromatisés et ne contenant aucun fruit).

[1187] V. par ex. CA Pau, ch. corr., 3 avr. 2008, arrêt préc. (a été sanctionné sur ce fondement un « marabout » promettant des miracles en cinq jours). – CA Douai, 13[e] ch., 29 sept. 2008, *Juris-Data* n° 2008-371368 (a été considérée comme trompeuse la publicité faisant la promotion de cabines de bronzage par UV et annonçant que les séances permettaient de protéger la peau contre l'exposition au soleil alors qu'il s'gait d'une information fausse selon un rapport de l'Organisation mondiale de la santé). – CA Lyon, ch. corr., 29 oct. 2008, *Juris-Data* n° 2008-371645 (a été sanctionné au titre de la publicité trompeuse une publicité ayant pour objet de promouvoir un désherbant présenté comme biodégradable et sans effet non nocif sur l'environnement).

[1188] Art. L. 121-1-1,18° C. conso.

[1189] Art. L. 121-1-1, 15° C. conso.

[1190] Art. L. 121-1-1, 16° C. conso.

[1191] Pour un exemple illustré, v. Lambert VERJUS, « Le *spamming* en question : Exemples illustrés et conseils pratiques », préc., spéc. pp. 22-23.

[1192] Pour un exemple de publicité trompeuse en matière de « pillules miracles » relevé par le Service Public Fédéral (SPF) belge, disponible sur :
http://statbel.fgov.be/fr/consommateurs/Internet/Spam/Facebook_pirate/index.jsp.

[1193] Art. L. 121-1-I, 2°, f) C. conso.

[1194] L'article L. 121-1-1 du Code de la consommation relatif aux pratiques réputées trompeuses renforce considérablement la répression des tromperies portant sur les qualités, aptitudes ou droits du professionnel : sont réputées trompeuses, les pratiques par lesquelles un professionnel se prétend « *signataire d'un code de conduite alors qu'il ne l'est pas* » (art. L. 121-1-1, 1° C. conso.) ou affiche « *un certificat, un label de qualité ou un équivalent sans avoir obtenu l'autorisation nécessaire* » (art. L. 121-1-1, 2° C. conso.), ou encore les pratiques résidant dans le fait « *d'affirmer qu'un code de conduite a reçu l'approbation d'un organisme public ou privé alors que ce n'est pas le cas* » (art. L. 121-1-1, 3° C. conso.) ; ou « *qu'un professionnel, y compris à travers ses pratiques commerciales, ou qu'un produit ou service a été agréé, approuvé ou autorisé par un organisme public ou privé alors que ce n'est pas le cas, ou de ne pas respecter les conditions de l'agrément, de l'approbation ou de l'autorisation reçue* » (art. L. 121-1-1, 4° C. conso.). L'article L. 121-1-1, 21° du Code de la consommation répute encore trompeuse la pratique consistant à « *faussement affirmer ou donner l'impression que le*

Dans le cadre du *spamming,* les messages de ce type se rencontrent fréquemment dans le secteur de l'éducation : des *e-mails* émanant de prétendues universités étrangères proposent une offre de formation diplômant totalement fictive [1195].

418. Au travers des exemples précités, on constate que le champ d'application particulièrement large de la catégorie relative aux allégations fausses ou trompeuses permettra de sanctionner de nombreux *spams* au contenu mensonger.

c. L'incertitude quant l'annonceur

419. L'article L. 121-1, I, 3° du Code de la consommation dispose que la pratique commerciale est trompeuse lorsque « *la personne pour le compte de laquelle elle est mise en œuvre n'est pas clairement identifiable* ». Or, très souvent, en matière de *spamming*, il est impossible pour les destinataires d'identifier l'auteur du message puisque ce dernier utilise fréquemment de fausses adresses ou des adresses usurpées afin d'échapper à toute traçabilité.

2. Les tromperies par omission

420. Présentation et effets en matière de *spamming*. D'une part, sont sanctionnées les omissions ou dissimulations portant sur des informations dites « substantielles » [1196]. Une information est qualifiée de substantielle dès lors qu'elle est de nature à influencer de façon déterminante le choix du consommateur. Celle-ci devient trompeuse lorsqu'elle est susceptible *« d'altérer de manière substantielle, le comportement économique* » du consommateur moyen [1197]. D'autre part, le nouvel article L. 121-1, II du

professionnel n'agit pas à des fins qui entrent dans le cadre de son activité commerciale, industrielle, artisanale ou libérale, ou se présenter faussement comme un consommateur ».

[1195] Pour un exemple illustré, V. Lambert VERJUS, « Le *spamming* en question – Exemples illustrés et conseils pratiques », préc., spéc. pp. 26 et 30.

[1196] Rappr. de l'article 1110 du Code civil qui dispose que : « [l']*erreur n'est une cause de nullité de la convention que lorsqu'elle tombe sur la substance même de la chose qui en est l'objet. Elle n'est point une cause de nullité lorsqu'elle ne tombe que sur la personne avec laquelle on a l'intention de contracter, à moins que la considération de cette personne ne soit la cause principale de la convention* ».

[1197] Art. L. 120-1, al. 1er C. conso. – Selon l'alinéa 2 du même article, certaines informations sont considérées par nature comme substantielles, à savoir : « *les caractéristiques principales du bien ou du service ; l'adresse et l'identité du professionnel ; le prix toutes taxes comprises et les frais de livraison à la charge du consommateur, ou leur mode de calcul, s'ils ne peuvent être établis à l'avance ; les modalités de paiement, de livraison, d'exécution et de traitement des réclamations des consommateurs, dès lors qu'elles sont différentes de celles habituellement pratiquées dans le domaine d'activité professionnelle concerné ; l'existence d'un droit de rétractation, si ce dernier est prévu par la loi* ». Dans ces circonstances, l'absence de l'un de ces éléments

Code de la consommation, issu de la loi du 3 janvier 2008, dispose qu'« *une pratique commerciale est également trompeuse si,* […] *elle omet, dissimule ou fournit de façon inintelligible, ambiguë ou à contretemps une information substantielle ou lorsqu'elle n'indique pas sa véritable intention commerciale dès lors que celle-ci ne ressort pas déjà du contexte* » [1198]. Cette exigence est particulièrement importante lorsque la pratique commerciale s'effectue par le biais de l'internet dans la mesure où il est souvent plus difficile d'identifier la nature commerciale ou seulement informative des offres transmises par *e-mail*. En matière de *spamming*, elle permet de renforcer l'obligation de transparence imposée par la LCEN [1199]. Surtout, cette nouvelle incrimination constitue un apport important puisqu'elle permet de pénaliser l'absence de certaines informations qui auparavant n'était sanctionnée que par le droit commun de la responsabilité civile. Tel était le cas, par exemple, de l'information portant sur les « *caractéristiques essentielles du bien ou du service* » [1200], « *sur les prix, les limitations éventuelles de la responsabilité contractuelle et les conditions particulières de la vente* » [1201]. Le nouveau texte relatif aux tromperies par omission apporte désormais à ces hypothèses une coloration pénale dont l'effet peut être particulièrement efficace si l'on considère que l'omission d'une information substantielle caractérisera automatiquement une tromperie, sans qu'il soit nécessaire d'évaluer au cas par cas les effets trompeurs de la pratique sur le consommateur moyen [1202]. En matière de *spamming*, le niveau lacunaire des informations contenues dans les *spams* permettra de les sanctionner aisément sur ce fondement.

3. Élément moral commun aux pratiques trompeuses

421. Jusqu'en 2009, le temps des incertitudes. À l'origine, la sanction du délit de publicité mensongère était subordonnée à la preuve de la mauvaise foi de l'auteur des actes incriminés [1203]. Sous l'empire de la loi n° 73-1193 du 27 décembre 1973 et avant le nouveau Code pénal, la transformation de cette infraction en délit de publicité trompeuse avait conduit la jurisprudence à abandonner l'exigence de mauvaise foi. La simple négligence ou imprudence découlant de l'absence de vérification de la sincérité ou de la véracité du message litigieux avant sa diffusion suffisait à caractériser l'élément moral du délit de

conduira les juges à en déduire le caractère trompeur de la pratique, sans même rechercher l'effet produit sur un consommateur moyen.

[1198] Art. L. 121-1, II, al. 1er C. conso.

[1199] V. *supra* : n° 304.

[1200] Art. L. 111-1 C. conso.

[1201] Art. L. 113-3 C. conso.

[1202] Nicolas ÉRESEO, *Pratiques commerciales trompeuses*, fasc. préc., spéc. n° 51.

[1203] Loi n° 63-628 du 2 juillet 1963 préc.

publicité trompeuse [1204]. Après l'entrée en vigueur du nouveau Code pénal, le caractère non intentionnel du délit de publicité fausse ou de nature à induire en erreur semblait perdurer. Dans un arrêt du 14 décembre 1994, la chambre criminelle de la Cour de cassation, avait clairement qualifié la publicité trompeuse de délit d'imprudence [1205]. Les lois de 2008 sont restées, quant à elles, silencieuses s'agissant de la caractérisation de l'élément moral des pratiques commerciales trompeuses. Bien qu'une partie de la doctrine estimait que la solution issue de la loi de 1973 avait de grandes chances de perdurer [1206], ce silence a suscité des hésitations d'interprétation [1207]. La jurisprudence était pour sa part divisée sur cette question : alors que certains juges retenaient le caractère intentionnel de ce type d'infraction tel qu'il avait été historiquement consacré [1208], pour d'autres au contraire, la simple négligence ou imprudence suffisait à caractériser un comportement délictuel punissable [1209]. Dans un arrêt du 15 décembre 2009, la chambre criminelle de la Cour de cassation a toutefois mis fin au flottement jurisprudentiel qui entourait la question de l'élément moral en qualifiant, sur le fondement de l'article 121-3 alinéa 1er du Code pénal, la pratique

[1204] Cass. crim., 4 déc. 1978, pourvoi n° 77-92.400 ; *Juris-Data* n° 1978-799342 ; *Bull. crim.* 1978, n° 342 ; *Gaz. Pal.* 9 mai 1979, 1, p. 129.

[1205] En ce sens, v. not. Cass. crim., 14 déc. 1994, pourvoi n° 92-85.557 ; *Juris-Data* n° 1994-002701 ; *Bull. crim.* 1994, n° 415 ; *JCP* 1995, éd. G., IV. 764 ; *Dr. pénal* avr. 1995, comm. 98, pp. 12-13, obs. J.-H. Robert ; *Rev. sc. crim.* 1995, p. 570, obs. B. Bouloc *; Rev. sc. crim.* 1995, p. 597, obs. J.-C. Fourgoux (la Cour de cassation ayant retenu, outre le caractère trompeur de la publicité incriminée, que la société n'avait pas vérifié « *la sincérité et la véracité du message publicitaire avant d'assurer sa diffusion* », la cour d'appel a justifié la condamnation du prévenu pour publicité fausse ou de nature à induire en erreur, ces « *motifs caractérisant* […] *la négligence du prévenu* »). – Cass. crim., 26 oct. 1999, pourvoi n° 98-84.446 , *Juris-Data* n° 1999-004316 ; *Bull. crim.*, n° 233 ; *Rev. sc. crim.* 2000, p. 384, obs. B. Bouloc ; *D.* 2000, AJ, p. 80 (« *l'élément moral du délit de publicité de nature à induire en erreur* […] *est caractérisé par une simple faute d'imprudence ou de négligence* »). – Cass. crim., 19 oct. 2004, pourvoi n° 04-82218, *Juris-Data* n° 2004-025542 ; *Bull. crim*. 2004, n° 245 (« *Attendu que les éléments matériel et moral du délit de publicité de nature à induire en erreur procèdent du seul caractère trompeur, qui peut résulter d'une faute de négligence ou d'imprudence, de l'un ou l'autre des éléments d'information, quel qu'en soit le support, donnée au client potentiel pour lui permettre de se faire une opinion sur les caractéristiques des biens ou services qui lui sont proposés* »).

[1206] V. en ce sens Jérôme LASSERRE CAPDEVILLE, « La substitution du délit de pratiques commerciales trompeuses au délit de publicité fausse ou de nature à induire en erreur », chron. préc., spéc. n° 39. – Emmanuel DREYER, « Un an de droit de la publicité », chron. préc., spéc. n° 3.

[1207] V. Stéphanie FOURNIER, « De la publicité fausse aux pratiques commerciales trompeuses », étude préc., spéc. note 45.

[1208] V. CA Pau, 18 sept. 2008, *Juris-Data* n° 2008-372637 – CA Chambéry, 2 juill. 2008, *Juris-Data* n° 2008-370873 (jugeant que la prévenue n'avait « *pas volontairement cherché à tromper le consommateur en attirant la clientèle avec une publicité comportant des indications qu'elle savait erronées* »). – CA Grenoble, 23 févr. 2009, *Juris-Data* n° 2009-377045).

[1209] V. par ex. CA Paris, 21 nov. 2008, *Juris-Data* n° 2008-005949 (en omettant de leur fournir l'« *information de nature à permettre aux acquéreurs profanes d'apprécier objectivement l'objet de la vente*, [la prévenue] *a commis, en tant que professionnel, une négligence qui suffit à caractériser la faute en dehors de toute intention de nuire* »). – CA Paris, 26 nov. 2008, *Juris-Data* n° 2008-374091. – CA Douai, 29 janv. 2009, *Juris-Data* n° 2009-376104 (« *s'agissant de l'élément moral, l'annonceur réalise l'infraction même s'il n'a pas eu l'intention de tromper : l'absence de mensonge est indifférente à la réalisation de l'infraction. Le délit de publicité trompeuse est donc un délit d'imprudence* ». – Pour d'autres exemples de décisions de juges du fond, v. Agathe LEPAGE, « Un an de droit pénal de la consommation (avril 2008-avril 2009) », chron. préc., spéc. nos 26 à 29. – Cass. Crim. 24 mars 2009, pourvoi n° 08-86.530, *Juris-Data* n° 2009-047943 ; *Dr. pénal* juin 2009, comm. 84, p. 34 et s., obs. J.-H. Robert ; *Cont. conc. conso.* août-sept. 2009, comm. 235, pp. 39-40, obs. G. Raymond (en l'espèce, il y avait pratique commerciale trompeuse dans le fait de ne pas avoir en disponible des articles objet d'une campagne publicitaire, la Cour de cassation jugeant ainsi que : « *la prévenue n'a pas veillé à la véracité du message publicitaire* »). – Cass. crim, 6 oct. 2009, pourvoi n° 08-87.757, *Juris-Data* n° 2009-05010171 ; *Dr. pénal* juin 2009, comm. 153, p. 37 et s., obs. J.-H. Robert.

commerciale trompeuse de délit intentionnel [1210]. Si dans la première partie de sa réponse au second moyen du pourvoi, la Cour de cassation a semblé consacrer la qualification de délit d'imprudence, en approuvant la cour d'appel d'avoir condamné le prévenu au motif que ce dernier « *n'*[avait] *pas pris toutes les précautions propres à assurer la véracité des messages publicitaires* », cette première qualification a néanmoins été rapidement évincée au profit de celle de délit intentionnel. La Haute juridiction a en effet explicitement jugé que « *la seule constatation de la violation, en connaissance de cause, d'une prescription légale ou réglementaire implique de la part de son auteur l'intention coupable* ». La solution est donc claire : le délit de pratiques commerciales trompeuses est un délit intentionnel ; l'élément moral est présumé et les juges du fond sont libérés de toute obligation de constater l'imprudence du prévenu. Cette solution est opportune puisque d'une part, elle a pour effet d'établir une cohérence avec des infractions proches comme la tromperie [1211] et l'escroquerie [1212] qui requièrent, en toute logique, une intention coupable [1213] et d'autre part, elle est respectueuse du principe de légalité, l'un des principes directeurs du droit pénal général [1214].

4. Poursuites et sanctions

422. Nature de l'infraction. Si le *spamming* peut être sanctionné au titre des pratiques commerciales trompeuses en raison de son contenu, se pose la question de savoir si le « spammeur » peut être sanctionné autant de fois qu'il existe de destinataires du même message. Par un arrêt du 8 décembre 1987, la Cour de cassation a jugé que « *le délit de publicité de nature à induire en erreur, même s'il se manifeste lors de chaque communication au public d'une telle publicité, constitue une infraction unique qui ne peut être poursuivie et sanctionnée qu'une seule fois dès l'instant où il s'agit d'allégations identiques, contenues*

[1210] Cass. crim. 15 déc. 2009, pourvoi n° 09-83.059 ; *Juris-Data* n° 2009-050976 ; *Bull. crim.*, n° 212 ; *D.* 2010, p. 203, note X. Depech ; *Dr. pénal* mars 2010, comm. 41, pp. 59-60, note J.-H. Robert ; *AJ Pénal* 2010, p. 73, note N. Éréséo et J. Lasserre Capdeville ; *Rev. sc. crim.* janv.-mars 2010, p. 146 et s., note C. Ambroise-Castérot.
[1211] Art. L 213-1 C. conso.
[1212] Art. 313-1 C. pén.
[1213] Art. 121-3 al.1er C. pén. – Approuvant l'arrêt de la Cour de cassation en considérant le choix opéré comme « *logique et rationnel* » (v. en ce sens, Coralie AMBROISE-CASTEROT, note sous Cass. crim. 15 déc. 2009, arrêt préc., *Rev. sc. crim.* janv.- mars 2010, p. 146 et s., spéc. p. 150).
[1214] En effet, selon ce principe, l'article 121-3, alinéa 1er du Code pénal dispose qu' « *il n'y a point de crime ou de délit sans intention de le commettre* », l'alinéa second précisant que le délit d'imprudence n'est constitué que « *lorsque la loi le prévoit* ». Pour qu'une infraction d'imprudence ou de négligence puisse exister, il est indispensable que la loi prévoie un contenu spécial relatif à l'élément moral. Or, la loi ne donne aucune précision à cet égard en matière de pratique commerciale trompeuse. Ce silence conduit dès lors à en déduire le caractère intentionnel de cette infraction.

dans le même message publicitaire et diffusées simultanément » [1215]. Il convient de préciser que cette solution n'est applicable que si la pratique commerciale s'adresse à un public indéterminé de consommateurs. La qualification de délit unique retenue découle directement de la mise en oeuvre de l'adage « *non bis in idem* » et évite ainsi que l'auteur d'une publicité trompeuse qui l'a adressée en de nombreux points du territoire ne soit poursuivi et sanctionné par les diverses juridictions territorialement compétentes. Le *spamming* constituera donc un délit unique chaque fois que les messages expédiés auront un contenu identique et seront destinés de façon aléatoire à un public, par nature, indéterminé. *A contrario,* la règle n'a plus vocation à s'appliquer en cas de « *publicités distinctes* […] *qui, adressées à des personnes différentes, mettent en scène de manière individualisée leurs destinataires, objet des allégations trompeuses* » [1216]. Il en est ainsi, par exemple, lorsque des « *brochures ont une forme et un contenu identiques,* [mais] *sont toutes individualisées par la citation et la mise en scène de chacune des personnes à qui elles étaient adressées* » [1217]. Dans cette hypothèse, « *il existe autant d'infractions que de personnes visées* » [1218]. Il en serait de même pour « *une annonce répétitive paraissant ou étant diffusée à plusieurs reprises pourrait entraîner des poursuites répétées* [ou pour un] *message qui serait modifié d'une parution ou d'une diffusion à l'autre* » [1219].

423. Sanctions pénales. De lourdes sanctions sont prévues, à savoir : une peine d'emprisonnement de deux ans et/ou une amende de 37.500 euros [1220], l'amende pouvant « *être portée à 50% des dépenses de la publicité ou de la pratique constituant le délit* » [1221]. Quant aux personnes morales reconnues coupables de cette infraction, l'article L. 121-6 alinéa 3 du Code de la consommation dispose qu'elles peuvent être sanctionnées d'une amende [1222] dont le taux maximum est égal au quintuple de celui prévu pour les personnes

[1215] Cass. crim., 8 déc. 1987, pourvoi n° 85-92.404; *Bull. crim.*, n° 451, p. 1194 ; *RTD com.* 1988, p. 668, obs. J. Hémard et B. Bouloc ; *Rev. sc. crim.* oct.-déc. 1988, p. 808, obs. J.-Cl. Fourgoux (dans cette espèce, la victime était toutefois unique, à savoir un concurrent de l'auteur de la publicité trompeuse). – V. dans le même sens en matière d'affiches et de tracts diffusés sur la voie publique, Cass. crim., 27 mars 2007, pourvoi n° 06-85.442 ; *Juris-Data* n° 2007-038470 ; *Bull. crim.*, n° 94 ; *Dr. pénal* juin 2007, comm. 87, obs. J.-H. Robert ; *D.* 2007, p. 1336, obs. C. Rondey. – Emmanuel DREYER, « Un an de droit de la publicité », chron. préc., spéc. n° 11.

[1216] Cass. crim., 30 janv. 1992, *Graeff*, *Bull. crim.* 1992, n° 44 ; *JCP* 1992, éd. E., pan. 829 ; *Dr. pénal* août-sept. 1992, comm. 208, pp. 13-14, obs. J.-H. Robert ; *RTD com*. 1992, p. 880, obs. P. Bouzat ; *RTD com*. 1993, p. 151, obs. B. Bouloc. – Cass. crim. 14 mars 2000, pourvoi n° 99-85.147. – Cass. crim. 17 oct. 2000, pourvoi n° 00-80.148.

[1217] Cass. crim., 30 janv. 1992, arrêt préc.

[1218] Cass. crim., 30 janv. 1992, arrêt préc.

[1219] Jean-Claude FOURGOUX, note sous Cass. crim., 8 déc. 1987, arrêt préc., *Rev. sc. crim.* oct.-déc. 1988, p. 808.

[1220] Art. L.121-6 C. conso. renvoyant à l'art. L. 213-1 du même Code.

[1221] Art. L.121-6, al. 2 C. conso. – Les personnes physiques peuvent également être condamnées à des peines complémentaires dont la publication du jugement (art. L. 121-4 C. conso.) et la diffusion à ses frais d'une ou plusieurs annonces rectificatives (art. L. 121-4 C. conso.).

[1222] Art. L. 213-6 C. conso.

physiques [1223]. Dans le cadre de la lutte contre le *spamming*, la sévérité de ces dispositions pourra se révéler un instrument de dissuasion satisfaisant, si tant est que ces dernières soient appliquées par les juges dans toute leur ampleur.

C. LE *SPAMMING*, SUPPORT DES PRATIQUES AGRESSIVES

424. Les pratiques commerciales agressives [1224] ont été créées par la loi du 3 janvier 2008 [1225] et sont venues élargir le champ des « pratiques commerciales déloyales » [1226]. Est ainsi sanctionné tout comportement qui consisterait à exercer une pression sur le consommateur, par le biais de « *sollicitations répétées et insistantes ou l'usage d'une contrainte physique et morale* », qui aurait pour effet d'« *altére*[r] *ou de nature à altérer de manière significative la liberté de choix du consommateur* » ou « *vicie*[r] *ou de nature à vicier le consentement* [de ce dernier] » ou encore d'« *entrave*[r] *ou de nature à entraver* [ses] *droits contractuels* » [1227]. Une pratique commerciale est considérée comme agressive dès lors qu'elle est de nature à fausser le consentement du consommateur et que ce résultat est la conséquence d'un fait de « *harcèlement, de contrainte, y compris la force physique ou d'influence injustifiée* » [1228]. Enfin, sont également réputées agressives les pratiques ayant pour objet « *de se livrer à des sollicitations répétées et non souhaitées par* […] *courrier électronique* » [1229], sous réserve que l'atteinte au libre choix du consommateur soit consécutive à des sollicitations « *personnalisées* » [1230]. Dans le cas du *spamming*, cette condition pourrait se vérifier lorsque le « spammeur » procède à un ciblage des destinataires avant tout envoi des messages. Tel est le cas notamment lorsqu'il se procure un fichier

[1223] Art. L. 131-38, al. 1er C. pén. – Les personnes morales peuvent également être condamnées à une ou plusieurs peines complémentaires, à savoir notamment « *l'interdiction, à titre définitif ou pour une durée de cinq ans au plus, d'exercer directement ou indirectement une ou plusieurs activités professionnelles ou sociales* » ou « *la fermeture définitive ou pour une durée de cinq ans au plus des établissements ou de l'un ou de plusieurs des établissements de l'entreprise ayant servi à commettre les faits incriminés* », à l'exclusion toutefois de leur dissolution (art. L. 131-39 C. pén.).

[1224] Cette expression n'est pas sans rappeler le titre d'une chronique rédigée par Jean CALAIS-AULOY en 1970 (« Les ventes agressives », *D.* 1970, chron., p. 37 et s.).

[1225] Art. 39 loi n° 2008-776.

[1226] V. not. Guy RAYMOND, « Les modifications au droit de la consommation apportées par la loi n° 2008-3 du 3 janvier 2008 pour le développement de la concurrence au service des consommateurs », étude préc., spéc. n° 35 et s. ; « Modifications au droit de la consommation », *in Présentation de la loi n° 2008-3 du 3 janvier 2008 pour le développement de la concurrence au service des consommateurs, J.-Cl. Conc.-Conso.*, Fasc. 10 – Actualités, 2008, n° 30 et s., spéc. nos 64 et s. – Stéphanie FOURNIER, « De la publicité fausse aux pratiques commerciales trompeuses », étude préc., spéc. n° 3.

[1227] Art. L. 122-11, al. 1er C. conso. – Philippe CONTE, « Brèves observations à propos de l'incrimination des pratiques commerciales agressives », étude préc.

[1228] Art. L. 122-11, al. 2 C. conso.

[1229] Art. L. 122-11-1, 3 C. conso.

[1230] Guy RAYMOND, « Les modifications au droit de la consommation apportées par la loi n° 2008-3 du 3 janvier 2008 pour le développement de la concurrence au service des consommateurs », étude préc., spéc. n° 37 ; « Modifications au droit de la consommation », fasc. préc., spéc. n° 66.

d'adresses électroniques regroupant des personnes sur un critère précis (selon leurs habitudes d'achat, leur localisation géographique, leur appartenance à une société ou à une association, etc.) ou encore lorsqu'un site marchand continuerait à expédier des messages publicitaires à un ancien client alors même que ce dernier n'aurait pas donné son consentement à recevoir de nouveaux courriers.

§ 3. LE *SPAMMING*, VÉHICULE D'INFRACTIONS SANCTIONNÉES PAR LE DROIT PÉNAL DE L'INFORMATIQUE

425. Le délit d'action frauduleuse sur les données : Élément légal. L'article 323-3 du Code pénal incrimine « [l]*e fait d'introduire frauduleusement des données dans un système de traitement automatisé ou de supprimer ou de modifier frauduleusement les données qu'il contient* ».

426. Élément matériel. La pratique incriminée doit être dirigée contre les données contenues dans un système : toute action portant sur des données extraites du système – par exemple, des données inscrites sur une disquette – échappe à cette disposition [1231]. S'agissant des actions visées, trois types de pratique sont punissables : l'introduction, la suppression et la modification de données [1232]. Introduire des données consiste à « *incorporer des caractères magnétiques nouveaux dans un support existant, soit vierge, soit contenant déjà d'autres caractères magnétiques* » [1233]. Il peut ainsi s'agir de l'insertion de caractères informatiques étrangers dans le système, tels que par exemple une bombe logique, un cheval de Troie ou un virus [1234]. La chambre criminelle de la Cour de cassation a sanctionné au titre de l'introduction volontaire de données inexactes dans un STAD une salariée, responsable du service informatique, qui avait saisi des mentions erronées quant au code du taux de TVA applicable [1235]. De même, s'est rendu coupable d'introduction frauduleuse de données dans le STAD du GIE cartes bancaires, le prévenu qui, après avoir manipulé et décrypté des données, avait inséré sur des cartes de nouvelles données capables de tromper le terminal de paiement [1236]. Contrairement à « *l'introduction de données* [qui] *est une opération*

[1231] V. Raymond GASSIN, *Informatique (fraude informatique)*, préc., spéc. n° 207.
[1232] Sur ces trois notions, v. notamment Raymond GASSIN, « La protection pénale d'une nouvelle " universalité de fait " en droit français : Les systèmes de traitement automatisé de données », art. préc., spéc. n° 180 et s., p. 39 et s.
[1233] Raymond GASSIN, citant J.- P. BUFFLELAN (« La protection pénale d'une nouvelle " universalité de fait " en droit français : Les systèmes de traitement automatisé de données », art. préc., spéc. n° 181, p. 39).
[1234] À propos de l'introduction d'un virus, v. CA Paris, 15 mars 1995, *Juris-Data* n° 020627 ; *JCP* 1995, éd. E., pan., p. 596 (en l'espèce, la relaxe a toutefois été prononcée, faute de preuve de l'élément moral).
[1235] Cass. crim. 5 janv. 1994, *JCP* 1994, éd. G., I. 359, spéc. n° 16, obs. M. Vivant et C. Le Stanc .
[1236] CA Paris, 9e ch. corr., sect. A, 6 déc. 2000, arrêt préc.

primaire » [1237], la suppression des données constitue « *une opération secondaire, car elle suppose l'existence préalable d'une opération d'introduction de données* » [1238]. Elle consiste à « *retrancher des caractères enregistrés sur un support magnétique par effacement de ceux-ci, ou* [à] *écrase*[r] *par surimpression de nouveaux caractères sur les anciens, ou encore par transfert et stockage des caractères à supprimer dans une zone réservée de mémoire* » [1239]. Le texte permet ainsi de réprimer toute manipulation ou suppression de données contenues dans un STAD ou encore leur déplacement hors du système. Enfin, la modification des données peut se manifester par une transformation de l'information qu'elles contiennent.

427. Élément moral. Le délit d'atteinte frauduleuse aux données suppose un dol général : l'agent doit avoir agi avec la conscience qu'il introduisait, supprimait ou modifiait des données contenues dans un système. Il doit avoir agi frauduleusement, c'est-à-dire en sachant que l'introduction, la suppression ou la modification des données n'était pas autorisée mais était déterminé à agir ainsi [1240]. Comme pour les délits d'accès, de maintien ou d'intrusion frauduleuse, l'élément moral réside dans la violation délibérée d'un interdit [1241]. Le délit de l'article 323-3 du Code pénal ne sera dès lors pas constitué si l'atteinte aux données contenues dans un système est consécutive à une erreur, une négligence ou une imprudence. La volonté de nuire n'est pas requise [1242].

428. Sanctions. Cette infraction est punie de cinq ans d'emprisonnement et de 75.000 euros d'amende [1243]. Enfin, la tentative est punissable au même titre que le délit lui-même [1244].

429. Quid du *spamming* ? Des études récentes montrent que les *spams* contiennent de plus en plus souvent des virus ou des *malwares* qui infectent les postes destinataires. Ces programmes informatiques malveillants peuvent porter atteinte aux données contenues dans le système victime de ces attaques en les supprimant, en les modifiant ou encore en y

[1237] Raymond GASSIN, « La protection pénale d'une nouvelle " universalité de fait " en droit français : Les systèmes de traitement automatisé de données », art. préc., spéc. n° 182, p. 39).
[1238] *Id.*
[1239] *Id.*
[1240] V. par ex. Cass. crim. 8 déc. 1999, pourvoi n° 98-84752, *Bull. crim.* 1999, n° 296 (« *le seul fait de modifier ou supprimer, en violation de la réglementation en vigueur, des données contenues dans un système de traitement automatisé [en l'espèce, un système comptable automatisé] caractérise le délit prévu à l'article 323-3 du Code pénal* »).
[1241] Jean DEVEZE, *Atteintes aux systèmes de traitement automatisé de données,* fasc. préc., spéc. n° 73. – Les délit d'accès, de maintien ou d'intrusion dans un sytème (entraver ou fausser) doivent être faits « *sans droit et en connaissance de cause* » (v. *supra* :n° 372 et).
[1242] Cass. crim., 8 déc. 1999, arrêt préc.
[1243] Art. 323-3 C. pén..
[1244] Art. 323-7 C. pén. issu de l'art. 46 loi n° 2004-575.

adjoignant de nouvelles données. Dans ce cas de figure, la preuve de l'élément moral ne pose pas de difficulté puisque le « spammeur » agit en sachant qu'il lui est pourtant interdit de procéder à de telles opérations sur le poste d'autrui. Toutefois, à notre connaissance, aucun « spammeur » n'a encore été sanctionné sur ce fondement.

*

* * *

430. Dans les hypothèses que nous venons d'examiner le *spamming* est exclusivement envisagé en tant qu'accessoire d'autres comportements illicites. Cependant, cette étude s'avère incontournable puisque ces cas de figure constituent des menaces très fréquentes sur le réseau. En effet, l'expérience démontre que le *spamming* apparaît sous des formes de plus en plus dangereuses soit en véhiculant des contenus destinés à tromper les destinataires des messages, soit en facilitant des fraudes dirigées contre les données. Dans ces conditions, la proximité entre le *spamming* et certaines agissements frauduleux tels que l'escroquerie, les pratiques déloyales ou encore l'action frauduleuse sur les données, imposait l'examen de chacune de ces infractions ainsi que les sanctions prévues dans la mesure où le succès de la lutte contre ces formes de *spamming* est étroitement lié à une répression efficace de ces comportements illicites.

CONCLUSION DU CHAPITRE 1

431. Cette étude a permis de mettre en évidence que le droit pénal pouvait intervenir de façon pertinente au soutien de la législation anti-*spam* en prenant en compte des comportements que cette dernière n'envisage pas. Tel est le cas du droit pénal de l'informatique qui permet de sanctionner le *spamming*, à la fois en tant qu'infraction autonome, lorsque celui-ci a pour effet de porter atteinte aux systèmes de traitement des données, mais également lorsqu'il est le vecteur d'actions frauduleuses sur les données numériques. L'intervention du droit pénal de la consommation se révèle en théorie intéressante pour sanctionner le caractère trompeur des *spams* commerciaux dans la mesure où la LCEN ne le traite pas. Cependant, en pratique, il est à déplorer qu'aucune action contre des « spammeurs » n'ait été, à ce jour, engagée sur ce fondement. Enfin, l'escroquerie permet, pour sa part, de réprimer de façon plus large les contenus trompeurs destinés à la remise d'informations identifiantes ou d'une somme d'argent et ce, quelle que soit leur finalité (commerciale ou non). Complément indispensable certes, le droit pénal reste néanmoins insuffisant pour permettre à l'ensemble des « spammés » d'engager une action contre le « spammeur » et s'imposer ainsi comme une réponse suffisante pour lutter contre le *spamming*. En effet, au regard des rares décisions intervenues, la responsabilité pénale du « spammeur » n'a été engagée dans le cas où le *spamming* est une infraction autonome, c'est-à-dire en cas d'atteintes aux systèmes de traitements automatisés des données. Ces hypothèses, nous l'avons vu, correspondent soit à une attaque de *mail bombing*, soit au cas celui où des ordinateurs sont contrôlés à distance à l'insu de leur propriétaire (PC zombie). Si le recours à ces deux techniques continue de sévir, une forte proportion de « spammeurs » échappe néanmoins à tout risque de poursuites faute d'action engagée par les « spammés ». On ne peut que déplorer cette sous-exploitation des instruments pénaux disponibles et ce constat est d'autant plus regrettable qu'ils pourraient avoir un réel effet dissuasif sur les « spammeurs ».

CHAPITRE SECOND : L'ACTION EN RESPONSABILITÉ CIVILE

432. L'envoi illicite de *spams* est susceptible de causer des dommages divers selon les destinataires : encombrement, voire saturation de la bande passante des FAI, engorgement des boîtes de messagerie des entreprises, atteinte aux données à caractère personnel, et dans certaines circonstances, perte de messages légitimes [1245]. Afin d'obtenir la réparation de leur préjudice, les victimes ont alors la possibilité d'engager une action en responsabilité civile délictuelle contre le « spammeur », fondée sur l'article 1382 du Code civil. Nous verrons que, dans la plupart des cas, la mise en œuvre de cette action ne pose pas de difficultés particulières. Pour autant, nous constaterons que ce type de recours est très rare en pratique [1246] alors qu'elle a, au contraire, dans une acception approchante, gagné les faveurs des juges américains. Dans certains cas, la victime et le « spammeur » auront noué des liens contractuels. Il en sera ainsi lorsqu'une personne souscrit un contrat de fourniture de service Internet et se livre par la suite à une activité de *spamming*, pourtant interdite dans ce type de contrat [1247]. Agissant alors en violation des termes du contrat conclu, cet abonné sera susceptible de voir sa responsabilité contractuelle engagée. Il apparaît donc que, selon la nature du rapport de droit existant entre le « spammeur » poursuivi et la victime, deux types d'actions en responsabilité sont envisageables : en l'absence de lien contractuel entre le « spammeur » et le « spammé », ce dernier pourra agir sur le fondement de la responsabilité délictuelle (Section I.) tandis que le FAI engagera une action en responsabilité contractuelle contre l'un de ses abonnés « spammeur » (Section II.).

[1245] Pour un exposé détaillé des dommages engendrés par le *spamming*, v. *supra* : n° 54 et s..

[1246] On dénombre à notre connaissance un arrêt qui se prononce sur le terrain de la responsabilité civile délictuelle, v. CA Paris, 25e ch. A., 28 févr. 2003, *Gaz. Pal.* 16 et 17 mai 2003, n° 137, p. 25 (jugeant que « *toute personne est recevable à se prévaloir de la faute quasi délictuelle qu'aurait commise une société d'édition en la harcelant par l'envoi de multiples courriers publicitaires personnalisés, aucune participation à un quelconque jeu ni à un achat n'étant nécessaires pour invoquer un préjudice moral lié à ce harcèlement* ». En l'espèce, les juges ont néanmoins considéré que « *l'intimé ne rapport*[ait] *pas la preuve ni d'une faute, ni d'un préjudice ; en effet, étant démontré que cette personne était abonnée au magazine édité par la société poursuivie et cliente de cette dernière, il était naturel que cette société cherche à faire connaître sa gamme de produits nouveaux et principalement à ses abonnés et clients, en leur adressant des mailings, comprenant une publicité promotionnelle pour un ou des produits ainsi que des jeux divers* »).

[1247] En effet, tout envoi de messages électroniques requiert au préalable une connexion à l'internet dont l'accès impose la conclusion d'un contrat avec un FAI et/ou fournisseur de messagerie.

SECTION I. LE *SPAMMING*, GÉNÉRATEUR DE RESPONSABILITÉ DÉLICTUELLE

433. Malgré la rareté des actions en responsabilité civile délictuelle engagée, le *spamming* constitue incontestablement un dommage pour les « spammés » qu'il convient de réparer. Il apparaît ainsi indispensable de s'interroger quant à l'opportunité d'un recours plus fréquent, en droit français, à la responsabilité délictuelle en matière de *spamming* (§ 2.). Toutefois, faute d'exemples jurisprudentiels permettant de déterminer concrètement comment les tribunaux ont apprécié les conditions d'engagement de la responsabilité délictuelle en matière de *spamming*, il nous est apparu pertinent de rechercher dans les droits étrangers proches de notre système de responsabilité civile délictuelle, de quelle façon les juges avaient apprécié la faute du « spammeur », le dommage qu'il avait causé, et le lien de causalité. À cet égard, le droit américain s'est révélé être un exemple particulièrement intéressant dans la mesure où il offre divers exemples d'application du droit de la responsabilité délictuelle (*tort law*) à la pratique du *spamming*. À plusieurs reprises, le *spamming* a été en effet poursuivi sur le fondement du *trespass to chattels* [1248], une théorie classique de la *Common law* qui peut se définir comme la dépossession ou l'interférence avec la possession ou le droit d'usage d'un tiers sur un bien meuble [1249] à l'origine d'un dommage [1250]. Si les conditions d'engagement de la responsabilité délictuelle exigées en droit américain et celles fixées en droit français ne sont pas strictement identiques, le *trespass to chattels* présente toutefois une structure proche de notre régime de responsabilité qui nous autorise à raisonner à partir de l'expérience américaine (§ 1.) [1251]. Trois conditions doivent notamment être réunies et que l'on retrouve classiquement en droit français, à savoir : une faute, un dommage et un lien de causalité [1252]. La confrontation des conditions de mise en œuvre de la responsabilité aux diverses hypothèses de *spamming* permettra ainsi d'apprécier l'efficacité de cette action et sera une occasion de repenser un droit de la responsabilité civile plus adapté aux spécificités du *spamming* (§ 3.).

[1248] *Restatement of the Law : Second, Torts*, American Law Institute Publishers St Paul, 1965, §218. – Le *Restatement* est une compilation purement académique réalisée par l'American Law Institute et dont l'autorité est simplement persuasive, et non impérative. – Sur l'histoire de cette doctrine : Richard A. EPSTEIN, " Intel v. Hamidi: The Role of Self-Help in Cyberspace? ", 1 *J. L . Econ. & Pol'y* 147, spéc. pp. 148-149 (2005).

[1249] Par abus de langage, on le traduirait par « l'entrée non autorisée aux biens meubles ». – Sur l'histoire de cette doctrine, v. Richard A. EPSTEIN, " Intel v. Hamidi : The Role of Self-Help in Cyberspace? ", 1 *J. L. Econ. & Pol'y* 147, spéc. 148-149 (2005) *(« ancient rule of trespass to chattels »).*

[1250] *Restatement (Second) of Torts* § 217 (1965).

[1251] Sur cette doctrine, v. par ex. Charlotte WAELDE (sous la dir.de), *Law and the Internet*, Hart Publishing, 2009.

[1252] Il convient de préciser que la responsabilité civile délictuelle aux États-Unis connaît une particularité par rapport au système français : une faute simple ne suffit pas à caractériser un *trespass*, ce dernier exigeant la preuve d'une faute intentionnelle. Le demandeur à l'action est donc tenu de démontrer que le *trespasser* a été animé de motifs illicites, c'est-à-dire d'une intention de nuire aux intérêts du propriétaire. Nous n'envisagerons toutefois pas cette condition dans notre étude dans la mesure où elle n'est pas requise en droit français (sur la question de l'intention en droit français, v. *infra* : n° 447).

§ 1. L'EXPÉRIENCE AMÉRICAINE COMME PISTE DE RÉFLEXION

434. Avant de voir comment le *trespass to chattels* a été adaptée au contexte de l'internet et plus particulièrement au phénomène du *spamming* (B.), il convient de définir plus précisément en quoi cette théorie ancienne présente une structure proche du régime de responsabilité français (A.)

A. LE *TRESPASS TO CHATTELS*, UNE STRUCTURE PROCHE DU REGIME DE RESPONSABILITE FRANÇAIS

435. La faute : Une dépossession ou une interférence. Le *trespass to chattels* est constitué dès lors qu'une personne est victime, soit d'une dépossession de son bien meuble, soit d'une entrave dans son utilisation [1253]. La dépossession couvre les circonstances dans lesquelles une personne prive une autre de la propriété de son bien meuble. Cette privation découle d'une absence d'autorisation préalable du propriétaire [1254] mais peut également résulter, par exemple, de la fraude, de la contrainte ou de la destruction du bien [1255]. À moindre effet, l'interférence est quant à elle constituée chaque fois que les intérêts du propriétaire sont altérés, dégradés ou diminués. Dans un premier temps, la jurisprudence a subordonné la preuve de l'interférence à l'existence d'un contact physique avec le bien meuble concerné [1256] pour ensuite se contenter d'un simple contact indirect [1257]. Progressivement, les juges sont allés encore plus loin dans cet assouplissement en reconnaissant que l'interférence était constituée alors même que le contact avait perdu de sa matérialité. Il a ainsi été jugé que des ondes sonores [1258], de la fumée [1259], ou encore des particules microscopiques provenant de traitements chimiques [1260] pouvaient être à l'origine d'un *trespass to chattels*. On constate ainsi que, bien avant l'avènement du cyberespace, les

[1253] *Restatement (Second) of Torts* § 217 (1965).
[1254] Et plus largement de l'usager légitime du bien.
[1255] *Restatement (Second) of Torts* § 221 (a.) (b.) (d.) (1965).
[1256] *Restatement (Second) of Torts* § 217 cmt. e. (1965).
[1257] Cette action a ainsi été admise lorsque des particules de ciment d'une usine avaient migré sur la propriété d'autrui (*Roberts v. Permanente Corp*., 188 *Cal. App. 2d*. 526, spéc. 529 ; (Ct. App. Jan. 26, 1961)).
[1258] *Wilson et al. v. Interlake Steel Co*. et al., 185 *Cal. Rptr*. 280, 32 *Cal.3d.* 229, spéc. 232-233 (Aug. 30, 1982) : la migration d'ondes sonores peut constituer un *trespass* dès lors qu'elle cause un dommage au bien et non un simple désagrément (*nuisance*) au propriétaire.
[1259] *Real v. Keen*, 838 *P.2d*. 1073, 314 *Or*. 370 (Or. 1992) (En l'espèce, un fermier qui avait brûlé ses champs, avait provoqué d'importantes fumées qui s'étaient répandues sur la propriété voisine. Les voisins l'avaient poursuivi en justice et la Cour suprême de l'Oregon, confirmant la décision de la cour d'appel de l'Oregon (*Real v. Keen*, 112 *Or.App*. 197, 828, *P.2d* 1038 (1992)), avait jugé que cette fumée s'était introduite sans permission, justifiant la demande de dommages et intérêts (*id.*, spéc. 1073, 1075).
[1260] *Bradley v. Am. Smelting & Refining. Co.*, 104 Wn.2d 677, spéc. 691, 709, *P.2d* 782 (Wash. 1985).

cours américaines avaient réduit à sa portion congrue la condition de contact physique, allègement propice à la transposition du *trespass* au contexte de l'internet.

436. Le dommage. Toute action fondée sur le *trespass to chattels* est subordonnée à la preuve d'un dommage. Une distinction s'opère selon le type de faute retenue. En cas de dépossession, cette dernière suffit à elle seule à retenir l'existence d'un dommage [1261]. En revanche, en cas d'interférence, le propriétaire doit rapporter la preuve que le bien meuble a été altéré quant à son état, sa qualité ou sa valeur, que le propriétaire a été privé de l'utilisation de son bien meuble pendant un temps substantiel [1262], que ce dernier a subi un dommage corporel ou encore que le prétendu intrus (*trespasser*) a nui à une personne ou une chose sur laquelle le propriétaire avait un intérêt légalement protégé [1263].

437. Lien de causalité. La responsabilité du *trespasser* est enfin subordonnée à la preuve de l'existence d'un lien de causalité entre la faute et le préjudice, cette existence s'appréciant au cas par cas.

438. Après cette première étude qui a permis de se familiariser avec la théorie américaine du *trespass to chattels*, il convient d'analyser comment s'est opéré le processus d'adaptation de cette théorie dans le contexte de l'internet.

B. LE PROCESSUS D'ADAPTATION DANS LE CONTEXTE DE L'INTERNET

439. Le renouveau d'une théorie classique. Les cours américaines ont progressivement ressuscité cette ancienne doctrine du *trespass to chattels* pour la transposer dans le contexte de l'internet afin d'y créer, au profit des FAI [1264], une sphère privative. La renaissance de cette théorie sous l'appellation doctrinale de « *cybertrespass* » [1265] visait ainsi à stopper un publipostage excessif qui engendrait des inconvénients croissants, non seulement techniques mais aussi financiers. L'amorce de ce processus s'est opérée pour la

[1261] *Restatement (Second) of Torts* § 218 cmt. d. (1965).
[1262] Pour évaluer le *quantum* du dommage subi dans ce cas, le demandeur devra prouver que l'interférence a perduré pendant une durée substantielle (*Restatement (Second) of Torts* § 218 cmt. i. (1965)).
[1263] *Restatement (Second) of Torts* § 218 (1965).
[1264] Si l'action fondée sur le *trespass to chattels* est ouverte à tout propriétaire d'équipements informatiques, on constatera que seuls les FAI l'ont mise en œuvre.
[1265] Sur l'évolution et l'application de cette doctrine aux nouvelles technologies, v. par ex. Mark D. ROBINS, " *Electronic Trespass: An Old Theory in a New Context* ", 15 *Computer Lawayer* 1 (1998). – Ashley L. ROGERS, Note, " *Is There Judicial Recourse to Attack Spammers ?* ", 6 *Vand. J. Ent. L. & Prac.* 338, spéc. pp. 340-345 (2004). – V. ég. Steven E. BENNETT, " *Canning Spam : CompuServe, Inc. v. Cyber Promotions, Inc.* ", 32 *U. Rich. L. Rev*. 545 (1998).

première fois dans le secteur des services téléphoniques dans une affaire où un fournisseur cherchait à obtenir la réparation de dommages consécutifs à des intrusions dans le système informatique de son réseau téléphonique (1.). Par la suite, l'application de cette théorie s'est étendue à la pratique du *spamming* (2.).

1. L'amorce

440. L'affaire *Thrifty-Tel, Inc. v. Bezenek*. Le *cybertrespass* a vu le jour dans le contexte des nouvelles technologies dans l'affaire *Thrifty-Tel, Inc. v. Bezenek* [1266]. En l'espèce, la société THRIFTY-TEL qui fournissait des services téléphoniques longue distance, attribuait à ses abonnés un code d'accès confidentiel leur permettant de passer des appels *via* son réseau informatique [1267]. Deux adolescents avaient réussi à pénétrer dans le réseau informatique de ce fournisseur grâce à un logiciel qui leur avait permis d'obtenir les codes d'accès nécessaires et de passer ainsi gratuitement des appels *via* le système de THRIFTY-TEL [1268]. L'exécution de ce programme pendant plusieurs heures avait généré plus de 1.300 appels automatisés ayant provoqué une surcharge du système qui rendait indisponible l'accès aux lignes téléphoniques pour les abonnés [1269]. C'est dans ce contexte que la société THRIFTY-TEL avait engagé une action sur le fondement du *trespass to chattels*.

441. Une appréciation souple des critères traditionnels. En réponse à la demande de THRIFTY-TEL, la cour d'appel de Californie s'était attachée à vérifier si les éléments constitutifs du *trespass to chattels* étaient réunis. S'inspirant de l'évolution très souple de l'exigence de contact physique avec le bien meuble [1270], la cour avait jugé que la réception de signaux électroniques générés par les activités des défendeurs était suffisamment tangible pour caractériser un contact physique et provoquer ainsi une interférence au sens de cette théorie [1271]. Quant au dommage, les juges avaient relevé que le programme de rappel automatique utilisé par les défendeurs avait surchargé le système

[1266] *Thrifty-Tel, Inc. v. Bezenek*, 46 *Cal.App. 4th* 1559, 54 *Cal.Rptr. 2d*. 468 (Cal.Ct. App. June 28, 1996). – Sur cette décision, v. Patricia L. BELLIA, " Defending Cyberproperty ", 79 *N.Y.U. L. Rev*. 2164, spéc. p. 2260 (2004). – Dan L. BURK, " The Trouble with Trespass ", 4 *J. Small & Emerging Bus L*. 27, 28 (2000). – Greg LASTOWSKA, " Decoding Cyberproperty ", 40 *Ind. L. Rev.* 23, spéc. pp. 25-26 (2006). – Adam MOSSOF, " Spam-Oy, What a nuisance ! ", 19 *Berkeley Tech. L.J*. 625, spéc. p. 641 (2004). – Laura QUILTER, Note, " The Continuing Expansion of Cyberspace Trespass to Chattels ", 17 *Berkeley Tech. L.J*. 421, spéc. pp. 428-428 (2002).
[1267] *Id*., spéc. 1564.
[1268] *Id*.
[1269] *Id*.
[1270] V. *supra* : n° 435.
[1271] *Id.*, spéc. 1567, n. 6: "*In our view, the electronic signals generated by the Bezenek boy's activities were sufficiently tangible to support a trespass cause of action*".

informatique de THRIFTY-TEL, empêchant ses abonnés d'accéder aux lignes téléphoniques [1272]. La cour avait ainsi retenu que s'était produite « *une interférence intentionnelle avec les biens mobiliers qui avait* […] *immédiatement provoqué un dommage* » [1273].

2. L'application du *trespass to chattels* au *spamming*

442. L'affaire *CompuServe, Inc. v. Cyber Promotions*. Le *cybertrespass*, tel qu'issu de la décision *Thrifty-Tel*, ne s'est pas limité au seul cas de piratage d'ordinateur mais s'est rapidement étendu aux activités liées à l'*e-mail*, en particulier à l'envoi de *spams* [1274]. À cet égard, mentionnons l'affaire *CompuServe v. Cyber Promotions*, première espèce en la matière, jugée devant la *U.S. District Court for the Southern District of Ohio* en 1997 [1275] et qui constitue et demeure la décision de référence sur laquelle d'autres cours fédérales se sont fondées par la suite pour traiter d'espèces similaires [1276].

443. Rappel des faits. À la suite de l'envoi par la société CYBER PROMOTIONS de millions de *spams* aux abonnés de la société COMPUSERVE, l'un des plus grands FAI américains, ce dernier avait reçu de très nombreuses plaintes de la part de ses clients, exaspérés par le volume inacceptable de *spams* reçus [1277]. Pour tenter de mettre un terme rapidement à cette situation, COMPUSERVE avait notifié aux défendeurs – CYBER PROMOTIONS et son président – une interdiction d'utiliser son équipement informatique à des

[1272] *Id.*, spéc. 1564 : "*Ryan's automated calling overburdened the system, denying some subscribers access to phones lines* ".
[1273] *Id.*, spéc. 1566.
[1274] Pour une étude générale du *spamming* et de l'emergence de jurisprudence en matière de *trespass to chattels*, Susan E. GINDIN, " Lost and Found in Cyberspace : Informational Privacy in the Age of the Internet", 32 *San Diego L. Rev*. 1153 (1997). – Anne E. HAWLEY, Comment, " Taking Spam Out of Your Cyberspace Diet : Common Law Applied to Bulk Unsolicited Advertising Via Electronic Mail ", 66 *UMKC L. Rev*. 381 (1997).
[1275] *CompuServe, Inc. v. Cyber Promotions, Inc.*, 962 *F. Supp*. 1015 (S.D. Ohio, Feb. 3,1997), arrêt préc. – Sur cette affaire, v. Mark D. ROBINS, " Electronic Trespass : An Old Theory in a New Context ", art. préc. – Steven E. BENNETT, " Canning Spam : CompuServe, Inc. v. Cyber Promotions, Inc. ", 32 *U. Rich. L. Rev*. 545 (1998). – Cette théorie a également été étendue au cas impliquant des *spiders*, des programmes automatiques qui cherchent des informations sur internet (v. not. *eBay, Inc., v. Bidder'sEdge, Inc.*, 100 *F. Supp.2d*. 1058 ((N.D. Cal. May 24, 2000). – *Register.com, Inc. v. Verio, Inc.*, 126 *F. Supp.2d.* 238, spéc. 241, 255 (S.D.N.Y., Dec. 12, 2000). – *Ticketmaster Corp. v. Tickets.com, Inc*. n° 99CV7654, 2000 WL 1887522, at *1 (C.D. Cal., Aug. 10, 2000). – Sur ces affaires, v. ég. Laura QUILTER, art. préc., spéc. p. 428.
[1276] Pour une espèce très similaire à l'affaire *CompuServe* v. *Am. Online, Inc., v. IMS et al., 24 F. Supp.2d* 548, spéc. 451-452 (E.D. Va., Oct. 29 1998) (citant à plusieurs reprises l'affaire *CompuServe*). – *Am. Online, Inc. v. National Health Care Discount, Inc.*, 121 *F. Supp.2d.* 1255, spéc. 1277 (N.D. Iowa, Sept. 29, 2000) (reconnaissant le *trespass* fondé sur l'envoi massif de *spams*, et citant l'affaire *Am. Online, Inc. v. IMS*, aff. préc.). – *Hotmail Corp. v. Van$ Money Pie Inc. et al.*, 47 *U.S.P.Q.2d.* 2010, 1998 WL 388389 (N.D. Cal., Apr. 16, 1998) (accordant une injonction après avoir jugé que l'envoi de *spams* depuis les comptes de FAI avait notamment endommagé le service d'*e-mails* de ce FAI).
[1277] *CompuServe*, 962 *F. Supp*., aff. préc., spéc. 1019. – V. ég. *IMS*, 24 *F. Supp.2d*., aff. préc., spéc. 550 (" *Both plaintiffs* [COMPUSERVE and AMERICAN ONLINE] *contended that they received complaints from subscribers* ").

fins d'envois de *spams* et leur avait demandé de cesser leurs activités qui encombraient son système informatique. En réaction, les défendeurs avaient riposté en multipliant les envois de *spams* aux abonnés de COMPUSERVE [1278]. Cette dernière avait alors eu recours à des mesures de filtrage destinées à détecter automatiquement et à bloquer tous les flux de transmission de messages provenant de CYBER PROMOTIONS [1279]. Cette défense avait toutefois été vaine puisqu'en réponse, les défendeurs avaient utilisé divers stratagèmes destinés à contourner le logiciel de dépistage utilisé par COMPUSERVE [1280]. Malgré les notifications renouvelées et les efforts de protection redoublés de COMPUSERVE [1281], CYBER PROMOTIONS avait poursuivi son activité. Face à cet entêtement, COMPUSERVE avait alors décidé de poursuivre CYBER PROMOTIONS sur le fondement du *trespass to chattels* afin d'obtenir à son encontre une injonction de cesser l'envoi de *spams* aux abonnés de COMPUSERVE [1282].

444. C'est donc à partir de cette décision de référence que nous exposerons, à l'occasion de l'étude de chacune des conditions de mise en œuvre de la responsabilité civile en droit français comment les juges américains ont concrètement caractérisé la faute du « spammeur » et le dommage subi consécutivement par le « spammé ».

§ 2. L'OPPORTUNITÉ D'UN RECOURS PLUS FRÉQUENT À LA RESPONSABILITÉ DÉLICTUELLE EN MATIÈRE DE *SPAMMING* ?

445. Contrairement au droit de la *Common law* où la responsabilité civile ne peut être engagée que si le comportement prétendu fautif correspond à l'un des délits (*torts*) expressément prévus par le système juridique [1283], le droit français définit de façon générale et abstraite le fait personnel de nature à engager la responsabilité civile de son auteur. En effet, l'article 1382 du Code civil, qui dispose que « [t]*out fait quelconque de l'homme, qui cause à autrui un dommage, oblige celui par la faute duquel il est arrivé, à le réparer* », fonctionne sur des modalités très générales qui sont la faute, le dommage et le lien de

[1278] *CompuServe* aff. préc., spéc. 1017, spéc. 1019. – V. ég. *IMS*, 24 *F. Supp.2d*., aff. préc., spéc. 550 (" *both* [COMPUSERVE and AMERICAN ONLINE] *contended that the bulk e-mailers continued to send messages even after they were notified that bulk e-mailing was unauthorized "*).
[1279] *CompuServe*, aff. préc., spéc. 1017-1019.
[1280] CYBER PROMOTIONS avait dissimulé la vraie origine de ses *e-mails*, en falsifiant les informations contenues dans les en-têtes des messages (*id.*, spéc. 1019). – Pour une affaire similaire, v. ég. *IMS*, 24 *F. Supp.2d*., spéc. 550.
[1281] *CompuServe*, aff. préc., spéc. 1019. – V. aussi *IMS*, 24 *F. Supp.2d*., aff. préc., spéc. 550.
[1282] *CompuServe*, aff. préc., spéc. 1017. – De son côté AOL demandait un jugement sommaire à l'encontre de IMS (*IMS*, 24 *F. Supp.2d*., aff. préc., spéc. 549) et de LCGM (*Am. Online, Inc. v. LCGM, Inc. et al*., Civ. Act. N° 98-102-A, 46 *F. Supp.2d*. 444, spéc. 446 (E.D. Va., Nov. 10, 1998).
[1283] Les différents *torts* constituent autant de cas spéciaux de responsabilité.

causalité [1284]. Appliqué au *spamming*, l'application de cette disposition suscite, tout comme celle du *trespass to chattels*, des interrogations quant à sa mise en œuvre. Au regard du triptyque traditionnel du droit de la responsabilité civile délictuelle, il conviendra de répondre successivement aux trois questions suivantes : comment se caractérise le comportement fautif du « spammeur » (A.) et le dommage causé par le *spamming* (B.) ?, comment les juges apprécient l'existence du lien de causalité (C.) ? Une fois que chacune des conditions de mise en œuvre de la responsabilité aura été analysée, il conviendra de traiter en dernière analyse la question de la réparation des « spammés » qui est en définitive l'objectif visé par tout « spammé » qui engage une telle action (D.).

A. LA QUESTION DU COMPORTEMENT FAUTIF DU « SPAMMEUR »

446. Après avoir défini la faute en droit positif français et ses applications au *spamming* (1.), nous déterminerons, de façon concrète, comment les cours américaines, confrontées à des affaires de *spamming*, ont caractérisé la faute commise par le « spammeur » (2.).

1. La faute en droit positif et ses applications au *spamming*

447. Définition et applications. La faute s'entend généralement comme la transgression d'un devoir préexistant [1285]. Certains auteurs préfèrent toutefois définir la faute comme une « *erreur ou une défaillance de conduite* » [1286]. L'existence de cet écart de conduite s'apprécie *in abstracto* à partir d'une analyse comparative entre l'attitude de l'auteur du dommage et celle qu'il aurait dû avoir « *par rapport à un modèle abstrait* » [1287]. Est donc en faute celui qui commet « *une erreur de conduite telle qu'elle n'aurait pas été*

[1284] Pour une étude comparative du droit de la responsabilité délictuelle en droit de la *Common law* et en droit français, v. par ex. Hadi SLIM, « Approche comparative de la faute dans la responsabilité civile extra-contractuelle », *Resp. civ. assur.* juin 2003, chron. n° 18, p. 59 et s.

[1285] Pour une étude générale de la faute, v. not. Patrice JOURDAIN, *Droit à réparation : Responsabilité fondée sur la faute. – Notion de faute : contenu commun à toutes les fautes*, *J.-Cl. Civil Code*, Fasc. 120-10, 2006.

[1286] Jacques FLOUR, Jean-Luc AUBERT, Éric SAVAUX, *Les obligations* : *Le fait juridique*, tome 2, 13e éd., Sirey, coll. *Sirey Université*, 2009, spéc. n° 98-1, p. 113.

[1287] Henri et Léon MAZEAUD et André TUNC, *Traité théorique et pratique de la responsabilité civile délictuelle et contractuelle*, (préf. Henri CAPITANT), tome 1, 6e éd., Montchrétien, 1965, spéc. n° 423, p. 494 et s. – Alain BENABANT, *Droit civil : Les obligations*, 12e éd., Montchrétien, coll. *Domat Droit privé*, 2010, spéc. n° 544, p. 388. – L'appréciation *in abstracto* consiste à apprécier la conduite de l'auteur du dommage par rapport au « bon père de famille ». Par opposition, l'appréciation *in concreto* s'opère par rapport à l'auteur lui-même et consiste à déterminer s'il a fait son possible au regard de ses aptitudes. – Pour une étude très approfondie de ces deux types d'appréciation, v. Noël DEJEAN DE LA BATIE, *Appréciation in abstracto et in concreto en droit civil français* (préf. Henri MAZEAUD), L.G.D.J., 1965.

commise par une personne avisée, placée dans les mêmes circonstances " externes " que l'auteur du dommage » [1288]. Toutefois, comme il a été mis en évidence par les professeurs Geneviève VINEY et Patrice JOURDAIN, l'opposition entre les deux définitions de la faute – acte illicite ou écart de conduite – concerne davantage les termes employés que le fond du droit. Quelle que soit la définition retenue, tous les auteurs s'accordent à dire que la faute consiste en la violation d'une norme imposée par le droit [1289]. La question se pose alors de savoir quelles sont les normes imposées par le droit et dont la violation caractérise une faute civile. Ces normes peuvent résulter d'une source formelle telle que la loi ou les règlements mais également d'une source informelle, à savoir d'« *une norme générale de conduite sociale imposant de se conduire en toutes circonstances avec prudence et diligence* » [1290]. C'est précisément cette définition qui, à l'occasion du rapport remis en 2005 au garde des Sceaux au nom de la Commission présidée par le professeur Pierre CATALA, et portant avant-projet de réforme du droit des obligations et de la prescription (« projet CATALA ») [1291], a été retenue : « [c]*onstitue une faute la violation d'une règle de conduite imposée par une loi ou un règlement ou le manquement à un devoir général de prudence ou de négligence* » [1292]. Par ailleurs, il convient de préciser qu'à la suite d'un important revirement de jurisprudence, toute personne, même dénuée de la capacité de discernement, peut être juridiquement responsable [1293]. Le droit positif consacre ainsi un*e conceptio*n objective de la faute [1294],

[1288] Henri et Léon MAZEAUD et André TUNC, *Traité théorique et pratique de la responsabilité civile délictuelle et contractuelle, op. cit.*, spéc. n° 439, p. 504. – V. ég. Alain BENABANT, *Les obligations, op. cit.*, spéc. n° 540, p. 385 (définissant la faute délictuelle comme « *une atteinte à l'attitude que l'on peut attendre entre concitoyens normalement conscients et respectueux de l'équilibre qu'exige toute vie en société* »). – Patrice JOURDAIN, *Droit à réparation : Responsabilité fondée sur la faute*, fasc. préc., spéc. n° 16-18. – Henri et Léon MAZEAUD, Jean MAZEAUD et François CHABAS, *Leçons de droit civil, Obligations : théorie générale*, tome 2, vol. 1, 9e éd., par François CHABAS, Montchrétien, 1998, spéc. n° 453, p. 466.

[1289] Sur cette controverse entre les partisans de l'illicéité et ceux soutenant la référence à l'écart de conduite, v. Geneviève VINEY et Patrice JOURDAIN, *Traité de droit civil : Les conditions de la responsabilité* (sous la dir. de Jacques GHESTIN), 3e éd., L.G.D.J., 2006, spéc. n° 441 et s., p. 363 et s. et les notes associées). Ces auteurs considèrent que « *l'opposition de la doctrine majoritaire qui fait de l'illicite un élément de la faute civile porte donc, à notre avis, sur la terminologie employée et non sur le fond du droit.* […] *qu'ils l'appellent " écart de conduite " ou " illicite ", tous les auteurs reconnaissent que la méconnaissance d'une norme imposée par le droit est indispensable à la construction d'une faute. Le désaccord signalé apparaît, par conséquent, superficiel et sans conséquences réelles sur la définition de la faute* » (*ibid., loc. cit.*).

[1290] Geneviève VINEY et Patrice JOURDAIN, *ibid.*, spéc. n° 450.

[1291] Avant-projet de réforme du droit des obligations et de la prescription, dit « projet CATALA », rapport au garde des Sceaux, 22 sept. 2005, Doc. fr. 2006. – Sur cet avant-projet, lire not. John CARTWRIGHT, Stefan VOGENAUER et Simon WHITTAKER (sous la dir.), *Regards comparatistes sur l'avant-projet de réforme du droit des obligations et de la prescription*, Société de législation comparée, coll. *Droit privé comparé et européen*, vol. 9, 2010.

[1292] Art. 1352 du projet. – Pour une critique de cette définition donnée par l'avant-projet, v. Jean-Sébastien BORGHETTI, « La définition de la faute dans l'avant-projet de réforme du droit des obligations », *in* John CARTWRIGHT, Stefan VOGENAUER et Simon WHITTAKER (sous la dir.), *Regards comparatistes sur l'avant-projet de réforme du droit des obligations et de la prescription, ibid.*, p. 295 et s. (l'auteur, critiquant la définition de la faute retenue comme « *exagérément large* » et qui renforce le caractère abstrait de la faute civile, regrette que le projet CATALA n'ait pas saisi l'occasion « *de doter le droit français de mécanismes qui permettraient d'encadrer la responsabilité civile de manière plus fine* » (*id.*, spéc. p. 308 et s.)).

[1293] Cass. Ass. plén., 9 mai 1984, pourvois n° 80-93.031 (arrêt *Lemaire*) et 80-93481 (arrêt *Derguini*) ; *JCP* 1984, éd. G., II. 20256, note P. Jourdain ; *D.* 1984, p. 525 et s., concl. J. Cabannes, note F. Chabas ; *RTD civ.* 1984, p. 508 et s., obs. H. Huet (« *la Cour d'appel, qui n'était pas tenue de vérifier si le mineur était capable de discerner les conséquences de son acte, a pu estimer sur le fondement de l'article 1382 du Code civil que la*

libérée de toute condition d'imputabilité et détachée de toute dimension moralisatrice [1295]. En matière de *spamming*, la preuve du comportement fautif du « spammeur » ne pose pas de difficultés puisque cette pratique a été très tôt condamnée par les usages de l'internet [1296] mais aussi par la CNIL [1297] alors même qu'aucune législation spécifique ne l'encadrait. Il semble dès lors que non seulement la collecte préalable d'adresses électroniques à l'insu de leur titulaire mais aussi l'envoi de *spams* caractérisent une faute civile.

2. L'appréciation de la faute du « spammeur » par les cours américaines

448. L'affaire *CompuServe*. Nous avons vu que la faute peut consister soit en une dépossession ou une interférence au sens du *Restatement (Second) of Torts*. Il convient dès lors à titre préalable de déterminer à quelle qualification correspond le *spamming*. Pour cela, rappelons que l'objectif premier des « spammeurs » n'est en aucun cas celui de s'approprier le réseau informatique du FAI mais de l'utiliser aux seules fins d'envois de *spams*. On constate ainsi que la pratique du *spamming* correspond à un *trespass to chattels* par interférence [1298]. Il appartenait alors aux juges de déterminer si l'expédition d'*e-mails* vers un serveur de messagerie pouvait constituer une interférence physique suffisante avec ce serveur, susceptible d'être poursuivie sur le fondement du *trespass to chattels*. Se référant au *Restatement (Second) of Torts* [1299], la cour de l'Ohio dans l'affaire *Compuserve* avait

victime avait commis une faute qui avait concouru, avec celle de M. Y…, à la réalisation du dommage dans une proportion souverainement appréciée »).

[1294] V. not. Henri et Léon MAZEAUD et André TUNC, *Traité théorique et pratique de la responsabilité civile délictuelle et contractuelle*, *op. cit.*, spéc. n° 424, p. 496 (la responsabilité civile « *est objective* […] *puisqu'il n'est plus question de tenir compte de l'état d'âme de l'auteur du dommage, mais seulement de comparer la conduite de celui-ci à la conduite d'un type abstrait* ». – Alain BENABANT, *Les obligations*, *op. cit.*, spéc. n° 545, p. 387 (« *La faute est devenue une notion purement objective, composée seulement d'un comportement de fait* [élément matériel : fait, comportement, attitude] *juridiquement qualifié d'anormal* [le même fait survenu dans les mêmes circonstances doit recevoir la même qualification juridique] *sans qu'il y ait à tenir compte de la psychologie de son auteur* [c'est-à-dire indépendamment de l'état de conscience de l'auteur du dommage] »).

[1295] L'imputabilité signifie que nul ne peut être juridiquement responsable s'il ne l'est pas moralement. La faute subjective est ainsi constituée de deux éléments : un comportement objectivement incorrect et une personne douée de discernement. Cette conception entraine alors l'irresponsabilité des personnes aliénées ou des enfants de bas âge (v. en ce sens, Jacques FLOUR, Jean-Luc AUBERT, Éric SAVAUX, *Le fait juridique*, *op. cit.*, spéc. n° 99 et s., p. 115 et s.). – Muriel FABRE-MAGNAN, *Droit des obligations : Responsabilité civile et quasi-contrats*, P.U.F., coll. *Thémis droit*, 2010, spéc. p. 96 et s. – Cette faute objective s'oppose ainsi à la faute pénale qui est, par définition, une faute subjective, cette dernière étant subordonnée à la preuve que l'auteur ait agi en pleine conscience de l'acte réalisé, c'est-à-dire qu'il en ait compris la nature et la portée (sur ce point, v. Bernard BOULOC, *Droit pénal général*, 21e éd., Dalloz, coll. *Précis*, 2009, spéc. n° 369, p. 326 et s.).

[1296] V. la Netiquette (v. *infra* : n° 507*)*

[1297] La CNIL a, dès 1999, dénoncé le *spamming* comme une pratique contraire à la directive du 24 octobre 1995 en raison de la collecte déloyale de la collecte de données (CNIL, *Le publipostage électronique et la protection des données à caractère personne*, rapport préc.).

[1298] Sur ce point, v. *CompuServe*, 962 *F. Supp*., aff. préc., spéc. 1021 (" *a trespass to chattels may be commited by intentionally using or intermeddling with the chattel in possession of another* "). – *IMS*, 24 *F. Supp.2d*., aff. préc., spéc. 550, *LCGM*, 46 *F. Supp.2d*., aff. préc., spéc. 452.

[1299] *Restatement (Second) Of Torts* § 217 cmt. e. (1965). – *CompuServe*, 962 *F. Supp*., aff. préc., spéc. 1021.

répondu par l'affirmative. Pour cela, elle avait adopté le raisonnement suivi par les juges dans l'affaire THRIFTY-TEL qui avaient retenu la condition du contact physique dans son acception la plus large [1300]. Elle avait ainsi établi une analogie entre les perturbations engendrées par la réception massive de *spams* qui avaient affecté la performance des systèmes informatiques de COMPUSERVE et celles provoquées par l'activité des garçons Bezenek dans l'affaire *Thrifty-Tel*. Ce rapprochement avait conduit les juges à décider que la transmission de signaux électroniques entre l'ordinateur incriminé de CYBER PROMOTIONS et le système informatique de COMPUSERVE, même en l'absence d'« interférence substantielle » avec le réseau de ce dernier, constituait un contact physique suffisant au sens du *trespass to chattels* [1301]. On le voit à travers cet exemple, il semble possible d'affirmer que les juges français, confrontés à une espèce similaire, suivront la même analyse qui apparaît, selon nous, tout à fait opportune.

449. L'indifférence quant à l'intention du fautif. La notion de faute soulève la question de savoir si l'engagement de la responsabilité de l'auteur du dommage est conditionné par l'intention qui l'anime comme c'est le cas en matière de *trespass to chattels* [1302]. La réponse est négative et découle de l'article 1383 du Code civil qui dispose que « *chacun est responsable du dommage qu'il a causé non seulement par son fait, mais aussi par sa négligence ou son imprudence* » [1303]. La responsabilité civile du présumé fautif peut donc être engagée même s'il n'a pas souhaité le résultat dommageable qui en a découlé. À ce titre, la Cour de cassation a clairement rappelé que « *l'application de l'article 1382 du Code civil n'exige pas l'existence d'une intention de nuire* » [1304]. Il semble donc que le droit français englobe davantage d'hypothèses de *spamming* que le *trespass to chattels* qui, pour sa part, requiert une intention de nuire [1305]. En pratique, cette solution est intéressante en matière de *spamming* car si l'on constate que le « spammeur » envoie toujours des messages

[1300] V. *supra* : n°s 440-441.
[1301] *CompuServe*, 962 *F. Supp*., aff. préc., spéc 1022 (citant l'affaire *Thrifty-Tel* se référant elle-même à l'affaire *Zaslow v. Kroenert*, 29 *Cal.2d* 541, 176 *P.2d* 1 (Cal.1946) (sur cette affaire, v. *supra* : n° 440)). – Dans le même sens, *LCGM*, 46 *F. Supp.2d*., aff. préc., spéc. 452 (citant l'affaire *CompuServe*, la *U.S. District Court for the Eastern District of Virginia* a jugé que le simple envoi de signaux électroniques au réseau d'AOL constituait un contact physique suffisant : " *The transmission of electrical signals through a computer network is sufficiently " physical " contact to constitute a trespass to property "*).
[1302] V. *supra* : n° 433.
[1303] Sur le rôle de l'intention, v. Aline VIGNON-BARRAULT, *Intention et responsabilité civile*, (préf. Denis MAZEAUD), P.U.A.M., coll. *Institut de Droit des Affaires*, 2004.
[1304] V. par ex. Cass. civ. 2e, 2 avr. 1997, pourvoi n° 95-14687; *Bull. civ.* II, n° 113.
[1305] V. *supra* : n° 433.

de façon volontaire, en revanche, il n'est pas systématiquement animé d'une intention de causer un dommage à son destinataire [1306].

B. LA QUESTION DU DOMMAGE CAUSE PAR LE *SPAMMING*

450. Après avoir défini d'une part le dommage en droit positif et ses possibles transcriptions en matière de *spamming* (1.) et d'autre part, les caractères requis pour que le dommage soit réparable (2.), il conviendra d'analyser comment les cours américaines, confrontées à des cas de *spamming*, ont caractérisé le dommage provoqué par cette pratique (3.).

1. Le dommage en droit positif et ses applications au *spamming*

451. Le dommage en droit français. Le droit français reconnaît deux types de dommage [1307] que l'on retrouvera en matière de *spamming* [1308]. Le dommage peut d'une part,

[1306] La preuve d'une intention de nuire pourrait être rapportée lorsque le « spammeur » entreprend par exemple une opération de *mail bombing* contre un FAI ou une société.

[1307] Nous utiliserons les termes de dommage et de préjudice comme synonymes, tel qu'ils sont le plus souvent considérés par la doctrine majoritaire. – V. en ce sens Jean CARBONNIER, *Droit civil : Les obligations, op. cit.*, spéc. n° 205, p. 377 (« *le dommage (ou préjudice), les deux mots sont synonymes* »). – V. ég. Yves CHARTIER, *La réparation du préjudice dans la responsabilité civile*, Dalloz, 1996, spéc. p. 1 (« *la distinction entre* [préjudice et dommage] *n'a pas vraiment de sens du point de vue juridique.* […] *Les deux termes peuvent être employés l'un pour l'autre* »). – Muriel FABRE-MAGNAN considère que « [l]*a distinction semble inutilement complexe.* […] *La distinction semble en outre dépourvue de conséquences juridiques* » (*Responsabilité civile et quasi-contrats, op. cit.*, spéc. p. 152). – Jacques FLOUR, Jean-Luc AUBERT, Éric SAVAUX, *Le fait juridique, op. cit.*, spéc. n° 133, p. 149 (« *un dommage – on dit, non moins couramment un préjudice* »). – Henri, Léon et Jean MAZEAUD et François CHABAS, *Leçons de droit civil, Les obligations : théorie générale*, tome 2, vol. 1, 9e éd. par François CHABAS, Montchrétien, 1998, spéc. n° 407, p. 412 (« *il n'est pas nécessaire de définir le préjudice car le sens juridique n'est autre que son sens courant* »). – Henri et Léon MAZEAUD et André TUNC, *Traité théorique et pratique de la responsabilité civile délictuelle et contractuelle, op. cit.*, spéc. n° 208, p. 261 (ces auteurs admettent également la synonymie des deux termes même s'ils font remarquer qu'à l'origine ils n'avaient pas le même sens (v. sur ce dernier point, *ibid.*, spéc. note 1, p. 261)). – Xavier PRADEL, *Le préjudice dans le droit civil de la responsabilité*, tome 415, L.G.D.J., coll. *Bibl. dr. privé*, 1995, spéc. n° 15, pp. 11-12 (« *il est assez regrettable d'isoler aussi drastiquement* […] *les éléments de faits et les éléments de droit. Si le préjudice est une notion de droit, encadrée par un certain nombre de règles juridiques, elle repose nécessairement sur une base factuelle.* […] *Cette distinction présente l'inconvénient de ne pas fournir de clé au juriste pour analyser les conséquences juridiquement réparables du dommage. De plus, si le dommage ne présente alors plus d'intérêt direct pour l'indemnisation de la victime, autant concentrer exclusivement l'analyse sur le préjudice, seule notion intéressante, car axée sur des situations concrètes. Voilà pourquoi, nous considèrerons* […] *que les termes de préjudice et de dommage peuvent être synonymes* ». – Geneviève VINEY et Patrice JOURDAIN, *Les conditions de la responsabilité, op. cit.*, spéc. n° 246-1. – *Contra* Philippe LE TOURNEAU (sous la dir.), *Droit de la responsabilité et des contrats*, 8e éd., Dalloz, coll. *Dalloz Action*, 2010, spéc. n° 1390, p. 451 (« *Pour penser rationnellement le droit de la responsabilité civile, il convient de le reconstruire à partir de la distinction des notions mêmes de dommage et de préjudice* […]. *Une chose est lésion, l'atteinte, celles des corps (dommage corporel), des choses (dommage matériel), des sentiments (dommage moral) ; autre chose sont les répercussions de la lésion, de l'atteinte, répercussions sur le patrimoine, répercussions sur la personne de la victime, sur ses avoirs (préjudice patrimonial) et sur son être (préjudice extrapatrimonial)* »). – V ég. Frédéric

consister en une atteinte au patrimoine, le dommage est alors dit matériel, patrimonial ou pécuniaire, c'est-à-dire « *directement susceptible d'évaluation pécuniaire* » [1309], et d'autre part, peut correspondre à une atteinte aux intérêts extrapatrimoniaux, c'est-à-dire « *qui ne porte aucune atteinte au patrimoine* » [1310], le dommage est alors dit moral ou extrapatrimonial [1311]. S'agissant des dommages matériels, la jurisprudence consacre une appréciation très souple des diverses formes que peut prendre ce type d'atteinte [1312]. Il peut tout d'abord s'agir d'une atteinte aux biens telle que la destruction, la détérioration ou la dépréciation d'un bien appartenant à la victime. Il peut encore s'agir d'une perte d'argent résultant de l'obligation d'exposer certains frais [1313], de la conclusion d'un contrat dans des conditions moins avantageuses que prévues, du non-paiement d'une somme d'argent, etc. [1314]. Enfin, est encore inclus dans cette catégorie le préjudice d'ordre économique qui « *naît de l'atteinte portée à l'activité économique d'une personne physique ou morale, c'est-à-dire à l'activité génératrice de revenus qu'elle mène* » [1315]. Concrètement, il correspond

---

BELOT, « Pour une reconnaissance de la notion de préjudice économique en droit français », *LPA* 28 déc. 2005, n° 258, p. 8 et s., spéc. p. 9 (qui souligne l'importance de distinguer ces deux notions, spécialement en matière de préjudice économique : « *un dommage corporel, par exemple, peut provoquer un préjudice économique, mais aussi des préjudices d'agréments pécunaire, physiologique, etc*. »). – Jean-Sébastien BORGHETTI, « Les intérêts protégés et l'étendue des préjudices réparables en droit de la responsabilité civile extra-contractuelle », *in Liber Amicorum, Études offertes à Geneviève VINEY*, L.G.D.J.-Lextenso, coll. *Les Mélanges*, 2008, p. 145 et s., spéc. p. 153 et s. (affirmant clairement que « *le préjudice juridique ne se confond pas avec le préjudice " factuel "* » et précisant que « *le dommage serait reconnu comme étant un élément purement factuel dont l'existence et la nature seraient du seul ressort de l'appréciation des juges du fond. Quant au préjudice, il serait ouvertement considéré comme constituant une notion juridique, ce qui permettrait d'expliquer que le préjudice, au sens du droit, ne coïncide pas toujours exactement avec les conséquences néfastes concrètes du dommage subi* »). – Le projet CATALA précité fait également la distinction entre le dommage « *désignant l'atteinte à la personne ou aux biens de la victime* » et le préjudice qui correspond à « *la lésion des intérêts patrimoniaux ou extra-patrimoniaux qui en résulte* » (spéc. note 19). – Comp. l'intérêt de cette distinction en droit pénal, v. Romain OLLARD, « La distinction du dommage et du préjudice en droit pénal », *Rev. sc. crim.* juill.-sept. 2010, p. 561 et s.

[1308] Il existe également un troisième type de dommage, le dommage corporel que nous n'évoquerons pas ici, son examen dépassant le dans le cadre de notre étude.

[1309] Jacques FLOUR, Jean-Luc AUBERT, Éric SAVAUX, *Le fait juridique, op. cit.*, spéc. n°135, p. 152.

[1310] Jean CARBONNIER, *Droit civil : Les obligations*, tome 4, *op. cit.*, spéc. n° 206, p. 380. – Yves CHARTIER, *La réparation du préjudice dans la responsabilité civile, op. cit.*, spéc. p. 35 (« *le préjudice moral, c'est avant tout celui que subit l'individu dans sa personne en dehors de toute blessure physique, et qui se traduit par une atteinte à des liens d'affection, à la réputation, à l'honneur, à l'image, à la vie privée* »).

[1311] Cette distinction apparaît, de façon très explicite dans le projet CATALA (v. proposition d'article 1343 du C. civ. : « *Est réparable tout préjudice certain consistant dans la lésion d'un intérêt licite, patrimonial ou extra-patrimonial* »).

[1312] Sur l'acception large de la notion de dommage matériel, v. not. Geneviève VINEY et Patrice JOURDAIN, *Les conditions de la responsabilité, op. cit.*, spéc. n° 251-1, pp. 30-31 (« *il n'y a pas lieu de distinguer entre l'atteinte à la valeur d'usage, c'est-à-dire la perte ou le trouble de jouissance, et la diminution de la valeur vénale desdits biens qui peuvent être des biens meubles ou immeubles, des biens corporels ou incorporels. Est également susceptible d'ouvrir droit à réparation le préjudice consistant dans l'impossibilité d'utiliser un bien pendant un certain temps* »).

[1313] V. par ex. CA Orléans, 23 oct. 1975, *JCP* 1977, éd. G., II. 18653, note Ph. Le Tourneau (frais d'exploitation auxquels une société d'autoroute a été exposée à la suite d'un accident dans la construction d'un édifice).

[1314] Geneviève VINEY et Patrice JOURDAIN, *Les conditions de la responsabilité, op. cit.*, spéc. n° 251-2, p. 31.

[1315] Frédéric BELOT, « Pour une reconnaissance de la notion de préjudice économique en droit français », doctr. préc., spéc. p. 8 ; « L'évaluation du préjudice économique », *D.* 2007, chron., p. 1681. – V. ég. Christian CYRIL VER HULST, « Dommage immatériel : du préjudice résultant des pertes d'exploitation », *LPA* 3 déc. 2001, n° 240, p. 4 et s. – En pratique et pour la doctrine majoritaire, les notions de « préjudice économique » et de « préjudice matériel » sont assimilées, confondues. — Christian LAPOYADE-DESCHAMPS définit le préjudice économique comme « *l'atteinte à un intérêt patrimonial, à titre principal, ou par répercussion d'un dommage à la personne ou d'un dommage aux biens* » (« La réparation du préjudice économique pur en droit français », *RIDC* 1998/2, p.

pour l'entreprise victime à une perte d'exploitation et « *est généralement qualifié de " perte d'une chance de réaliser une plus-value "* » [1316]. S'agissant du dommage moral [1317], malgré les nombreuses controverses très largement exposées sur la question du caractère indemnisable ou non du préjudice extrapatrimonial [1318], la jurisprudence française , s'accorde en principe à l'admettre [1319] et même très largement [1320].

452. Les transcriptions du dommage en cas de *spamming*. Pour certaines des victimes de *spamming*, le dommage subi s'analysera en un préjudice d'ordre économique. Il pourra en être ainsi tout particulièrement lorsqu'un « spammeur » mal intentionné souhaite nuire à sa victime en la « bombardant » d'*e-mails* non sollicités. Dans ce cas, l'envoi massif de *spams* risque d'engendrer une perturbation du serveur de messagerie de l'entreprise victime ou la saturation de la bande passante d'un FAI, lequel ne pourra plus assurer le bon fonctionnement de ses services de messagerie. Ils subiront l'un et l'autre un manque à gagner résultant notamment de la perte clients ou d'abonnés mécontents de tels dysfonctionnements techniques et d'une atteinte à leur réputation commerciale [1321]. En revanche, les « spammés », simples particuliers, pourront difficilement se plaindre d'un quelconque

367 et s., spéc. p. 367). – *Contra* Yvaine BUFFELAN-LANORE et Virginie LARRIBAU-TERNEYRE l'érigeant en un chef de préjudices à part entière : « *il ne faut surtout pas confondre le préjudice économique et le préjudice patrimonial qui concerne, d'une façon plus générale, toute atteinte au patrimoine, aux biens* » (*Droit civil : Les obligations*, 12e éd., Dalloz Sirey, 2010, spéc. n° 1641, p. 561 »). – Dans le même sens, v. Frédéric BELOT, « Pour une reconnaissance de la notion de préjudice économique en droit français », doctr. préc., spéc. p. 10 (« *les notions de " préjudice patrimonial " et " préjudice économique " nous semblent très différentes, car le patrimoine thésaurise les revenus alors que l'activité économique les crée* »).

[1316] Yvaine BUFFELAN-LANORE et Virginie LARRIBAU-TERNEYRE, *Droit civil : Les obligations*, *op. cit.*, spéc. n° 1641, p. 561.

[1317] Sur le préjudice moral, v. Olivier BERG, *La protection des intérêts incorporels en droit de la réparation des dommages : Essai d'une théorie en droit français et allemand*, (préf. Geneviève VINEY), Bruyland-L.G.D.D.J., 2006. – François GIVORD, *La réparation du préjudice moral*, thèse Grenoble, 1938.

[1318] V. not. Jacques FLOUR, Jean-Luc AUBERT, Éric SAVAUX, *Le fait juridique*, *op. cit.*, spéc. n° 140, p. 161. – Philippe LE TOURNEAU, *Droit de la responsabilité et des contrats*, *op. cit.*, spéc. n° 1551, p. 516. – Philippe MALAURIE, Laurent AYNES et Philippe STOFFEL-MUNCK, *Droit civil : Les obligations*, 4e éd., Defrénois, 2009, spéc. n° 248, p. 141 et s. – Henri et Léon MAZEAUD, Jean MAZEAUD et François CHABAS, *Obligations : théorie générale*, *op. cit*, spéc. n° 417 et s., p. 422 et s. – Henri et Léon MAZEAUD et André TUNC, *Traité théorique et pratique de la responsabilité civile délictuelle et contractuelle*, *op. cit.*, spéc. n° 292 et s., p. 392 et s. – Boris STARK, Henri ROLAND et Laurent BOYER, *Obligations : Responsabilité délictuelle*, tome 1, 5e éd., Litec, 1996, spéc. no 114 et s., p. 66 et s.

[1319] À cet égard, Alain BENABANT observe que le principe de réparation du préjudice moral est admis depuis le XIXe siècle et a « *pris une grande ampleur avec le développement des " droits de la personnalité ", droits dont la violation se traduit une réparation pécuniaire. Il faut ajouter qu'on conçoit aujourd'hui des formes de réparation adaptées à ce type de préjudice, comme par exemple des publications destinées à rectifier une atteinte commise par voie de presse* » (*Les obligations*, *op. cit.*, spéc. n° 673, p. 480). – V. ég. François TERRE, Philippe SIMLER et Yves LEQUETTE, Droit civil : *Les obligations*, 10e éd., Dalloz, coll. *Précis droit privé*, 2009, spéc. n° 712, pp. 726-727 (« *La jurisprudence a décidé que le dommage réparable pouvait être moral ce qui lui a notamment permis d'affirmer la responsabilité de son auteur en cas d'atteinte à l'honneur, la considération d'une personne y compris morale* »). – Sur la détermination des préjudices moraux indemnisables, v. Geneviève VINEY et Patrice JOURDAIN, *Les conditions de la responsabilité*, *op. cit.*, spéc. n° 255 et s., p. 39 et s.

[1320] La jurisprudence a admis qu'une simple angoisse pouvait être être indemnisable (en ce sens, v. CA Versailles, 4 févr. 2009, *D.* 2009, p. 819, obs. M. Boutonnet ; *JCP* 2009, éd. G., actu. 83, obs. C. Bloch, et *idem.*, I. 248, spéc. n° 3, obs. Ph. Stoffel-Munck (la cour d'appel a ordonné le retrait d'une antenne de téléphonie mobile afin de faire cesser « *le préjudice moral résultant de l'angoisse* » des voisins).

[1321] Cass. civ. 2e, 7 oct. 2004, pourvoi n° 02-14399.

préjudice pécuniaire dans la mesure où il est rare qu'un même *spam* soit envoyé deux fois à la même personne ; le « spammeur » opérant généralement à l'aide d'un logiciel de *push* qui permet un envoi simultané de *spams* à un très grand nombre d'adresses électroniques. Ces derniers pourraient alors invoquer un préjudice moral résultant d'une atteinte à la protection des données à caractère personnel pour l'exploitation de leurs données sans leur consentement ou d'une atteinte à leur droit à être laissé tranquille en raison de la gêne occasionnée par la réception d'un *e-mail* non sollicité ou de la perte ou du retard dans l'acheminement de leurs messages légitimes [1322]. Il est néanmoins permis de douter du succès d'une demande d'indemnisation pour ce type de dommage dans la mesure où la jurisprudence a tendance à refuser d'accorder une réparation pour les préjudices minimes [1323]. Deux hypothèses toutefois sont susceptibles de permettre au « spammé », simple particulier, d'obtenir l'indemnisation du préjudice subi. D'une part, lorsqu'il sera victime d'une attaque de *mail bombing* ; la saturation de sa messagerie électronique qui en résultera l'empêchera d'envoyer et de recevoir des *e-mails* et pourra ainsi constituer un dommage réparable [1324]. De même, dans le cas où son ordinateur, infecté par un virus devient un relai de *spams,* le dommage subi sera susceptible d'ouvrir droit à réparation. En effet, dans ce cas de figure, devenant à son insu un « spammeur », il pourra s'exposer à la réception de tous les *e-mails* qui lui seront retournés par les destinataires mécontents, provoquant ainsi la saturation de sa boîte électronique et l'impossibilité de profiter pleinement des fonctionnalités des services de messagerie (envoi/réception d'*e-mails*) [1325].

2. Les caractère du dommage réparable

453. Caractères personnel, direct, actuel et certain. Que le dommage allégué soit de nature patrimoniale ou extrapatrimoniale, ce dernier ne sera indemnisable que s'il est

[1322] À noter toutefois, qu'en matière d'atteinte aux droits de la personnalité, la mise en œuvre du droit commun de la reponsabilité de l'article 1382 du Code civil est « *aménagée* » (v. sur ce point, Caroline GAUVIN, « Les sanctions de droits de la personnalité : Une étude de droit civil », *Comm. com. électr.* mars 2004, p. 14 et s., spéc. n° 12, p. 17 : « *toute atteinte aux* [droits de la personnalité] *donne lieu à réparation, sans que la victime ait à prouver l'existence d'un dommage comme l'exige les règles classique de la responsabilité* (*id.*, spéc. n° 1). *Malgré cette particularité, il convenait de définir les dommages subis dans la mesure où « Si le principe de la réparation découle de la simple constatation d'une atteinte, l'évaluation des dommages et intérêts restent, quant à elle, liée à la gravité du préjudice.* […] *toute atteinte à un droit de la personnalité ouvre droit à réparation, la recherche du préjudice est nécessaire pour évaluer le quantum. Dans bien des cas, une motivation détaillée des dommages subis par la victime accroît le montant de la réparation tant il est vrai que les juges aiment à se rattacher à des éléments bien concrets. L'autonomie des droits de la personnalité au regard des droits de la personnalité est finalement plus apparente que réelle* » (*id.*, spéc. n° 9, p. 16)).

[1323] Sur ce point, v. *infra* n° 462 et s.

[1324] V. ég. *infra* : n° 455.

[1325] V. ég. *infra* : n° 455.

personnel, direct, actuel et certain [1326]. Il importe peu que celui-ci soit prévisible [1327] tant qu'il résulte d'un intérêt légitime, c'est-à-dire qu'il ne soit contraire ni aux lois ni aux bonnes mœurs [1328]. Cette dernière exigence ne suscitant pas d'observations particulières, nous concentrerons nos développements sur les quatre autres caractères précités conditionnant le droit à indemnisation. Le caractère personnel du dommage implique que seule la personne qui en a souffert peut en demander réparation [1329], ce qui en matière de *spamming*, ne pose pas de difficultés particulières. Quant au caractère direct, il se déduit du lien de causalité [1330]. Il s'agit pour le juge de déterminer si le dommage allégué est directement causé par la personne que la victime désigne comme fautive [1331]. S'agissant du caractère actuel requis, celui-ci signifie que le préjudice doit pouvoir être évalué au jour où le juge statue. Le préjudice réparable comprend celui qui s'est déjà produit mais aussi le dommage futur, lorsque sa réalisation en est certaine [1332], c'est-à-dire qu'il peut être quantifiable de façon précise lors du jugement. En définitive, le caractère certain apparaît comme la condition centrale de l'existence d'un préjudice. Pour que cette condition soit vérifiée, il faut que le juge soit convaincu que la victime ait subi un dommage. Il en sera ainsi toutes les fois où ce dernier se sera déjà produit au moment où le juge statuera. Cette exigence découle directement de l'application du principe selon lequel le montant de la réparation octroyé à la victime ne doit jamais aboutir à un enrichissement de cette dernière [1333]. Le caractère certain ainsi défini connaît toutefois des assouplissements. La jurisprudence a en effet admis qu'un dommage, même futur, peut ouvrir droit à réparation dès lors que sa survenance future n'est pas purement éventuelle mais apparaît « *comme la prolongation certaine et directe d'un état*

[1326] Jean CARBONNIER, *Droit civil : Les obligations*, tome 4, *op. cit.*, spéc. n° 205, pp. 377-379. – Si en théorie, ces caractères sont requis pour tous dommages quelle que soit leur nature, la jurisprudence ne les a originairement précisés que pour le dommage matériel ; l'analyse étant difficilement transposable dans le cas d'un dommage moral. Il en est ainsi tout particulièrement en ce qui concerne le caractère certain puisque ce dernier ne peut être qu'approximatif dans la mesure où il peut varier selon la sensibilité de la victime considérée (v. sur ce point Jacques FLOUR, Jean-Luc AUBERT, Éric SAVAUX, *Le fait juridique, op. cit.*, spéc. n° 134, p. 151 et n° 141, p. 163). – Pour des exemples d'arrêts qui n'ont pas vérifié l'ensemble de ces caractères, v. not. Cass. civ. 2e, 5 oct. 1988, *Gaz. Pal.* 1988, 2, pan., p. 270 ; *ibid.* 1989, 2, somm., p. 371, obs. F. Chabas (refus d'indemniser le préjudice moral en se bornant à constater son inexistence sans autres motivation). – Cass. civ. 2e, 4 juill. 1990, *Juris-Data n°* 1990-003025 ; *Resp. civ. assur.* nov. 1990, spéc. n° 357, obs. H. Groutel ; *Gaz. Pal.* 1990, 2, pan., p. 233 (a cassé l'arrêt de la cour d'appel qui a subordonné l'indemnisation du préjudice moral à son caractère exceptionnel).

[1327] En revanche, en matière de responsabilité contractuelle, la réparation ne s'étend qu'aux dommages « *qui ont été prévus ou qu'on a pu prévoir lors du contrat* » (art. 1150 C. civ).

[1328] Jean CARBONNIER, *Droit civil : Les obligations*, tome 4, *op. cit.*, spéc. n° 205, p. 379. – V. projet CATALA préc., proposition d'article 1343 du C. civil : « *Est réparable tout préjudice certain consistant dans la lésion d'un intérêt* licite ».

[1329] V. Geneviève VINEY et Patrice JOURDAIN, *Les conditions de la responsabilité, op. cit.*, spéc. pp. 118-124.

[1330] V. Samuel RETIF, *Droit à réparation : Conditions de la responsabilité délictuelle. – Le dommage. – Caractères du dommage réparable, J.-Cl. Civil Code, Art. 1283 à 1286*, Fasc. 101, 2005, spéc. n° 65 (« *le caractère direct du dommage constitue moins un caractère du dommage réparable que le lien de causalité nécessaire entre le dommage et le fait générateur du dommage* »).

[1331] Toutefois, les juges ont tendance à apprécier l'existence d'un lien de causalité de façon souple (sur ce point et ses applications en matière de *spamming*, v. *infra* : n° 461).

[1332] Sur la possible indemnisation du dommage futur, v. *infra :* n° 453.

[1333] Jacques FLOUR, Jean-Luc AUBERT, Éric SAVAUX, *Le fait juridique, op. cit.*, spéc. n°s 136-137, p. 154.

des choses actuel et comme susceptible d'évaluation immédiate » [1334]. Cette rédaction est reprise dans la proposition de loi de 2010 portant réforme de la responsabilité civile et qui suggère que l'article 1384 du Code civil soit ainsi rédigé : « *Est réparable* [... le] *préjudice futur, lorsqu'il est la prolongation certaine et directe d'un état de chose actuel* » [1335].

454. Caractère certain et perte de chance. L'exigence du caractère certain conduit également à s'interroger la possible indemnisation de la perte d'une chance [1336]. Définie comme « *la perte de l'espoir raisonnable d'un avantage futur* » [1337], la perte d'une chance est indemnisable dès lors que celle-ci est sérieuse [1338]. En effet, « *afin d'éviter que,* […]*, les rêves ne soient indemnisés comme des réalités* » [1339], « [l]*e fait que la chance soit constitutive du préjudice n'altère en aucune manière les mécanismes du droit de la responsabilité civile.* […] *Celui-ci doit répondre aux conditions de tout préjudice désignant un élément constitutif de la responsabilité civile, être actuel et certain, direct et légitime* » [1340]. À ce titre, la Cour de cassation a ainsi jugé que « *seule constitue une perte de*

[1334] Cass. civ. 2e, 15 déc. 1971, pourvoi n° 70-12603 ; *Bull. civ.* II, n° 345 ; *JCP* 1972, éd. G., IV, n° 30 ; *D.* 1972, somm., p. 96. – Cass. civ. 2e, 9 nov. 1972, *Bull. civ.* II, n° 276 ; *JCP* 1972, éd. G., IV. 294. – Le projet CATALA précité reprend à son compte cette jurisprudence fermement établie et précise que « *le préjudice futur est réparable lorsqu'il est la prolongation certaine et directe d'un état de chose actuel* » (proposition d'article 1345, al. 1er C. civil). – Sur la réparation du préjudice futur mais certain, v. not. Geneviève VINEY et Patrice JOURDAIN, *Les conditions de la responsabilité, op. cit.*, spéc. no 277 et s., pp. 84-87.

[1335] Laurent BETEILLE (présnetée par), Proposition de loi portant réforme de la responsabilité civile, Doc Sénat n° 657, 9 juillet 2010, disponible sur : http://www.senat.fr/leg/ppl09-657.pdf. – V. déjà en ce sens, projet CATALA préc., art. 1345. : « *Le préjudice futur est réparable lorsqu'il est la prolongation certaine te directe d'un état de chose actuel* ».

[1336] Pour une étude d'ensemble de la notion de perte de chance, v. Caroline RUELLAN, « La perte de chance en droit privé », *RRJ* 1999-3, p. 729 et s. – Jacques BORE, « L'indemnisation pour les chances perdues : une forme d'appréciation quantitative de la causalité d'un fait dommageable », *JCP* 1974, éd. G., I. 2620 (« *le préjudice certain, relatif à la faute commise n'étant que la perte d'une chance de réussite* » (*id.*, spéc. n° 7), « *chanc*[e] *sérieus*[e] *d'obtenir l'avantage escompté* » (*id.*, spéc. n° 34 et s.)). – Jérôme HUET, « Perte de chance : du plus ou moins classique », *RTD* civ. 1986, p. 117 et s. – Philippe MALAURIE, Laurent AYNES et Philippe STOFFEL-MUNCK, *Les obligations, op. cit.*, spéc. n° 242, p. 135 (« *La perte de chance n'est réparable que si elle est sérieuse c'est-à-dire s'il est probable que l'évènement heureux aurait pu se réaliser* »). – Sur la distinction entre la perte de chance et du risque de dommage, v. Loïs RASCHEL, note sous Cass. civ. 1re, 14 janv. 2010, pourvois n° 08-16.760 et 08-21.562 ; *Juris-Data* n° 2010-051047 ; *JCP* 2010, éd. G., note 413, p. 763 et s. – Geneviève VINEY et Patrice JOURDAIN, *Les conditions de la responsabilité, op. cit.*, spéc. no 278, p. 87 et s.

[1337] Caroline RUELLAN, « La perte de chance en droit privé », art. préc., spéc. n° 18, p. 737 et n° 21, p. 738 (« *Si l'espoir est réel et non éventuel, sa disparition constitue un "réel" préjudice, qui s'analyse en l'impossibilité de mener une évolution à son terme, en une incapacité définitive de transformer l'espérance en une issue espérée* »).

[1338] Jacques BORE, « L'indemnisation pour les chances perdues : une forme d'appréciation quantitative de la causalité d'un fait dommageable », art. préc. (« *le préjudice certain, relatif à la faute commise n'étant que la perte d'une chance de réussite* » (*id.*, spéc. n° 7), « *chanc*[e] *sérieus*[e] *d'obtenir l'avantage escompté* » (*id.*, spéc. n° 34 et s.)). – V. ég. Philippe MALAURIE, Laurent AYNES et Philippe STOFFEL-MUNCK, *Les obligations, op. cit.*, spéc. n° 242, p. 135 (« *Entre le dommage futur et certain réparable et le dommage éventuel qui ne l'est pas se trouve la perte de chance* […]. *La perte de chance n'est réparable que si elle est sérieuse c'est-à-dire s'il est probable que l'évènement heureux aurait pu se réaliser* »).

[1339] Philippe MALAURIE, Laurent AYNES et Philippe STOFFEL-MUNCK, *Les obligations, op. cit., loc. cit.*, spéc. n° 242, p. 135.

[1340] Caroline RUELLAN, « La perte de chance en droit privé », art. préc., spéc. n° 26, p. 740. – Pour une analyse approfondie sur le sujet, v. not. Jacques FLOUR, Jean-Luc AUBERT, Éric SAVAUX, *Le fait juridique, op. cit.*, spéc. n° 138, pp. 156-158. – Samuel RETIF, *Droit à réparation*, fasc. préc., spéc. n° 37 et s.

chance réparable, la disparition actuelle et certaine d'une éventualité favorable » [1341]. La perte d'une chance a, par exemple, été considérée comme indemnisable lorsque celle-ci concernait la perte d'une chance de gagner à un jeu de hasard, d'une réussite professionnelle, ou encore la perte d'une chance de se présenter à un examen ou à un concours [1342], la perte d'un espoir de promotion professionnelle [1343] ou d'entreprendre une nouvelle carrière, etc. [1344].

455. Perte de chance et *spamming.* Transposée au *spamming*, cette hypothèse pourrait se traduire, par exemple, par la perte d'une chance pour une entreprise victime d'une attaque de *mail bombing* d'obtenir la conclusion d'un contrat avantageux avec un nouveau client ou l'un de ses partenaires commerciaux [1345] ou de poursuivre un tel contrat [1346] en raison du dysfonctionnement de ses services de messagerie. De la même façon, ce type d'attaque pourrait exposer un internaute à la perte d'une chance de consulter un *e-mail*

[1341] Cass. civ. 1re, 21 nov. 2006, pourvoi n° 05-15674 ; *Bull. civ.* I, n° 498 ; *JCP* 2006, éd. G., IV. 3475 ; *JCP* 2007, éd. G., I. 115, spéc. n° 2, obs. P. Stoffel-Munck. – V. ég. Cass. crim. 4 déc. 1996, pourvoi n° 96-81.163 ; *Juris-Data* n° 1996-005343 ; *Bull. crim.* 1996, n° 445 ; *JCP* 1995, éd. G., IV. 720 (« *l'élément de préjudice constitué par la perte d'une chance présente un caractère direct et certain chaque fois qu'est constatée la disparition, par l'effet de l'infraction, de la probabilité d'un évènement favorable* »). – *Contra* par ex. Cass. civ. 2e, 9 nov. 1983, *Bull. civ.* II, n° 175 ; *JCP* 1985, éd. G., II. 20360, note Y. Chartier (cassation d'un arrêt d'appel qui a alloué à un enfant de neuf ans victime d'un accident, en plus de l'indemnité destinée à réparer une incapacité permanente partielle, une rente en réparation du préjudice subi pour perte de chance d'accéder à une situation bien rémunérée « *sans préciser en quoi la perte de chance retenue était certaine et en relation directe avec le fait dommageable* »). – Cass. crim., 23 sept. 2003, *inédit, Juris-Data* n° 2003-020922, pourvoi n° 02-84623 (la prétendue perte de chance alléguée par une maquilleuse, victime d'un accident de la circulation a été rejetée au motif qu'elle ne rapportait pas la preuve d'avoir été contrainte de renoncer à exercer à nouveau cette profession). – Cass. civ. 3e, 28 juin 2006, pourvoi n° 04-20040 ; *Bull. civ.* III, n° 164 ; *RTD civ*. 2006, p. 770, obs. P. Jourdain (jugeant qu' « *une faute commise dans l'exercice du droit de rupture unilatérale des pourparlers pré-contractuels n'est pas la cause du préjudice consistant dans la perte d'une chance de réaliser les gains que permettait d'espérer la conclusion du contrat* »).

[1342] v. par ex. TA Rennes, 6 juill. 1994, *LPA* 24 févr. 1995, p. 12 et s., note F. Mallol (une étudiante qui a été irrégulièrement ajournée à un examen à la suite d'une erreur de l'administration a subi un préjudice indemnisable dès lors qu'elle démontre la perte d'une chance sérieuse d'obtenir un emploi dès l'obtention de son diplôme). – *Contra* Cass. civ. 2e, 10 oct. 1973, pourvoi n° 72-12867 ; *Bull. civ.* II, n° 254 (refus d'indemniser le préjudice né de l'interruption d'une thèse de doctorat au motif que la victime ne justifiait pas du retentissement que cette interruption avait pu avoir sur la profession qu'elle envisageait d'exercer).

[1343] Cass. civ. 2e, 9 juill. 1954, *D.* 1954, jurispr., p. 627 (constitue un dommage certain indemnisable la perte de l'aptitude d'un fonctionnaire à être nommé à un grade supérieur). – *Contra* Cass. civ. 2e, 25 oct. 2001, *inédit*, pourvoi n° 99-16942 ; *Juris-Data* n° 2001-011536 ; *Resp. civ. assur.* janv. 2002, comm. 12, p. 16 (refusant d'indemniser une perte de chance d'obtenir une promotion professionnelle faute d'établir la preuve d'une chance réelle de promotion puisque « *postuler pour une promotion et même remplir les conditions de celle-ci ne permet pas à coup sûr d'affirmer que cette promotion aurait eu lieu* »).

[1344] Pour de très nombreux exemples de manifestations jurisprudentielles en faveur de l'indemnisation de la perte d'une chance, v. not., Geneviève VINEY et Patrice JOURDAIN, *Les conditions de la responsabilité*, *op. cit*., spéc. n° 280, p. 91 et s. – Pour plus de détails sur l'indemnisation de la perte de chance, v. *infra* : n° 465.

[1345] Cass. civ. 2e, 18 déc. 1963, *Bull. civ*. II, n° 845 (à propos de la perte de chance de trouver un acquéreur). – Cass. com., 3 mai 1979, *Bull. civ*. IV, n° 137 (à propos de la perte d'une chance d'obtenir le marché Gaz de France qui était un client important de la société victime).

[1346] Cass. crim., 16 janv. 1980, pourvoi n° 79-91793, *Bull. crim*. 1980, n° 25 ; *D*. 1980, I.R., p. 409, obs. C. Larroumet ; *JCP* 1980, éd. G., IV. 124 (jugeant que la cour d'appel avait méconnu le principe de réparation intégrale « *en refusant de tenir compte de ce que l'infraction en mettant obstacle à l'exécution normale du contrat de location de véhicules* [avait] *privé les parties civiles des avantages qu'elles étaient fondées à en attendre en contrepartie des sommes qu'elles avaient déjà versées et qui ne correspondaient que pour partie au coût de la location* »).

important qui n'aurait jamais pu être acheminé en raison de la réception massive de *spams*. En effet, l'encombrement de sa boîte électronique pourrait le priver d'une chance sérieuse d'obtenir un poste en raison de l'impossibilité de prendre connaissance d'un message l'invitant à se présenter à un entretien d'embauche. Cette perte de chance pourrait également caractériser un dommage réparable lorsque l'ordinateur de la victime a été transformé en PC zombie, les messages expédiés depuis ce poste à l'insu de son propriétaire et retournés massivement à cette même adresse par les destinataires mécontents pouvant entraîner la saturation de sa boîte de réception. Il convient toutefois de préciser qu'en dehors de ces deux hypothèses – *mail bombing* et PC zombie –, et dans le cas le plus fréquent où le « spammeur » envoie le même message à un nombre important de destinataires, l'indemnisation semble impossible dans la mesure où un seul *spam* ne peut encombrer une boîte aux lettres électroniques. En définitive, il apparaît que tout est une question d'espèce : plus le dommage est éloigné physiquement et chronologiquement de la faute et plus la victime devra s'attacher à prouver de façon scrupuleuse le lien de causalité qui les relie.

3. L'appréciation du dommage par les cours américaines

456. L'appréciation du dommage par les cours américaines. Rappelons à ce stade de l'analyse qu'en cas d'interférence, la responsabilité du *trespasser* peut être engagée si la victime rapporte la preuve de l'existence de l'un des trois dommages suivants : l'altération du bien meuble quant à son état, sa qualité, ou sa valeur, la privation du propriétaire de l'utilisation de son bien meuble pendant un temps substantiel ou un dommage corporel causé au propriétaire, ou encore un dommage produit sur une personne ou une chose sur laquelle le propriétaire a un intérêt légalement protégé [1347]. En l'espèce, la cour avait retenu deux dommages distincts subis par COMPUSERVE, à savoir : l'atteinte à l'état, la qualité ou la valeur du bien et le dommage occasionné à un bien sur lequel le propriétaire avait un intérêt légalement protégé.

457. L'atteinte à l'état, la qualité ou la valeur du bien. Afin de rechercher l'existence éventuelle d'un dommage, la cour de l'Ohio partait du constat que la valeur du système informatique de COMPUSERVE résidait dans sa capacité à répondre aux attentes de ses abonnés [1348]. Or, la réception massive de *spams* affaiblissait fortement cette capacité

[1347] *Restatement (Second) of Torts* § 218 (1965).
[1348] *CompuServe*, 962 *F. Supp.*, aff. préc., spéc. 1022 (" *In the present case, any value COMPUSERVE realizes from its computer equipment is wholly derived from the extent to which that equipment can serve its subscriber base* ").

puisqu'une partie du système informatique de COMPUSERVE était mobilisée pour retourner les *e-mails* ou stopper les futurs messages entrants de CYBER PROMOTIONS [1349]. En effet, le fait pour CYBER PROMOTIONS de déguiser l'origine de ses messages ralentissait leur traitement dans la mesure où les serveurs de COMPUSERVE étaient contraints de stocker un volume anormalement important d'*e-mails*. De surcroît, ces *e-mails* ne pouvaient être renvoyés faute d'adresse d'expéditeur valide. Ainsi, ces envois multiples utilisaient une partie de l'espace de stockage du système de COMPUSERVE et diminuait sa puissance de traitement, de sorte que ses ressources étaient insuffisantes pour satisfaire les demandes courantes de ses clients [1350]. Dans ces circonstances, la cour avait jugé que, bien que l'équipement informatique de COMPUSERVE n'avait pas été pas physiquement endommagé, la perturbation de son fonctionnement avait été suffisamment importante pour constituer un dommage [1351].

458. Atteinte à un intérêt légalement protégé. Pour reconnaître que COMPUSERVE avait subi une atteinte à un intérêt légalement protégé, à savoir sa réputation commerciale [1352], les juges de l'Ohio avaient relevé que l'indisponibilité totale ou partielle de ses ressources avait réduit l'utilité de son service de courrier électronique et avait ainsi incité de nombreux clients à mettre fin à leur abonnement [1353]. Toutefois, avant de retenir

[1349] *Id*. spéc. 1022.

[1350] *Id.*, spéc. 1022 (" *defendants' multitudinous electronic mailings demand the disk space and drain the processing power of plaintiff's computer equipment, those resources are not available to serve COMPUSERVE subscribers* " – V. ég. *IMS*, 24 *F. Supp.2d*., aff. préc., spéc. 550 (Selon la *U.S. District Court for the Eastern District of Virginia :* " *Both* [COMPUSERVE and AMERICAN ONLINE] *plaintiffs alleged that processing the bulk e-mail cost them time and money and burdened their equipment* "). – *LCGM*, 46 *F. Supp.2d*., aff. préc., spéc. 452 (la *U.S. District Court for the Eastern District of Virginia* citant en substance l'affaire *CompuServe*). – V. ég. *Van$ Money Pie Inc.*, aff. préc. 1998 WL 388389, spéc. *7, 37 ("[tens of thousands of misdirected e-mail messages] *fill*[ed] *up Hotmail's computer storage space and threaten*[ed] *to damage Hotmail's ability to service its legitimate customers* ").

[1351] *CompuServe*, 962 *F. Supp.*, aff. préc., spéc. 1022 (" *Therefore, the value of that equipment to CompuServe is diminished even though it is not physically damaged by defendants' conduct* "). – V. ég. *IMS*, 24 *F. Supp.2d*., aff. préc., spéc. 550 (" *Melle's contact with AOL's computer network* […] *diminished the value of its possessory interest in its computer network* "). – Dans le même sens, v. *LCGM*, 46 *F. Supp.2d*, aff. préc., spéc. 452 (citant *CompuServe*, 962 *F. Supp.* aff. préc., spéc. 1022 et le *Restatement (Second) of Torts* § 218 (b) : " O*ne who commits a trespass to chattel is liable to the possessor of the chattel if the chattel is impaired as to its "condition, quality, or value* ").

[1352] *CompuServe*, 962 *F. Supp.* aff. préc., spéc. 1023 ("*Defendants' intrusions into CompuServe's computer systems, insofar as they harm plaintiff's business reputation and goodwill with its customers, are actionable under Restatement § 218(d)* "). – V. ég. *IMS*, aff. préc., spéc. 550 (" *Melle's contact with AO 's computer network injured AOL's business goodwill* "). – V. ég. *Van$ Money Pie Inc.*, aff. préc., 1998 W.L. 388389, spéc. *7, 37 (" *that defendants' acts of trespass have damaged Hotmail* […] *in terms of harm to Hotmail's business reputation and goodwill "*).

[1353] Comp. *Intel Corp. v. Hamidi*, 30 *Cal. 4th* 1342, 71 *P.3d* 2961, 1 *Cal.Rptr. 3d*. 32 (June 30, 2003) (dans cette affaire, les juges ont refusé de reconnaître un dommage économique car le prétendu dommage invoqué par la société INTEL victime ne résultait pas de l'envoi massif d'*e-mails* comme dans l'affaire *CompuServe* mais du contenu des messages, ces derniers contenant des critiques à l'encontre d'INTEL (*id*., spéc. 41 :" *In sum, no evidence suggested that in sending messages through Intel's Internet connections and internal computer system Hamidi used the system in any manner in which it was not intended to function or impaired the system in any way. Nor does the evidence show the request of any employee to be removed from Face- Intel'smailing list was*

l'existence d'un tel dommage, la cour s'était également attachée à vérifier que COMPUSERVE avait mis en place des moyens technologiques d'auto-assistance raisonnables pour protéger ses systèmes [1354], ce que la demanderesse avait effectué à plusieurs reprises mais en vain [1355]. L'installation des moyens techniques semblait dès lors constituer pour la cour une condition supplémentaire pour fonder une action sur le fondement du *cybertrespass*. À tout le moins, cette exigence attestait que les juges exigeaient un certain niveau de diligence de la part des FAI avant de conclure définitivement à l'existence d'un dommage.

459. La controverse quant à la prise en compte des intérêts économiques. À l'aune de cette décision, le raisonnement adopté par la cour semblait démontrer que celle-ci s'était attachée aux dommages économiques les plus indirects, à savoir : la perte de confiance des clients à l'égard de COMPUSERVE et l'atteinte à son image et à sa réputation commerciale. Or, c'est sur ce point précis, à savoir la détermination du dommage dans son sens large, qu'ont porté les critiques de la doctrine américaine [1356]. Parmi les détracteurs, le Professeur Dan L. BURK soutient que dans la mesure où le délit de *trespass to chattels* protège un intérêt possessoire, une telle action doit être subordonnée à la preuve, non pas d'un dommage considéré globalement – encombrement des boîtes des abonnés, mécontentement de clientèle, perte de cette dernière et image de marque compromise – mais d'un dommage affectant le bien lui-même, c'est-à-dire le serveur de messagerie traitant les communications non désirées [1357]. En d'autres termes, le raisonnement adopté par la cour conduit, selon lui, à rompre le lien direct entre l'intérêt possessoire du demandeur et le dommage [1358]. Toutefois, force est de reconnaître que la prise en compte du dommage économique présente le mérite de ne pas exclure certains préjudices qui sont incontestablement provoqués par le *spamming.* Cette acception large du dommage s'inscrit dans l'esprit du cyberespace, monde systémique plus que hiérarchique. Elle permet en effet de protéger les FAI contre cette pratique qui engendre, dans la plupart des cas, de graves

not honored. The evidence did show, however, […] *that Intel technical staff spent time and effort attempting to block the messages* ").

[1354] *CompuServe*, 962 *F. Supp.*, aff. préc., spéc. 1023 (" *Sufficient legal protection of the possessor's interest in the mere inviolability of his chattel is afforded by his privilege to use reasonable force to protect his possession against even harmless interference*").

[1355] *CompuServe*, 962 *F. Supp*., aff. préc., spéc. 1021-24. – V. ég. *LCGM*, 46 *F. Supp.2d* 444, aff. préc. – *IMS*, 24 *F. Supp.2d*, spéc. 550-51.

[1356] Dan L. BURK, " The Trouble with Trespass ", art. préc., spéc. p. 53 (2000). – V. ég. Niva ELKIN-KOREN, " Let the Crawlers Crawl : On Virtual Gatekeepers and the Right to Exclude Indexing ", 26 *U. Dayton L. Rev.* 179, spéc. pp. 203–207 (2001). – Dan HUNTER, " Cyberspace as Place and the Tragedy of the Digital Anticommons ", 91 *Cal. L. Rev*. 439, spéc. pp. 483–488, (2003). – R. Clifton MERRELL, Note, " Trespass to Chattels in the Age of the Internet ", 80 *Wash. U. L. Q*. 675, spéc. pp. 687–697 (2002). – Maureen A. O'ROURKE, " Property Rights and Competition on the Internet : In Search of an Appropriate Analogy ", 16 *Berkeley Tech. L.J*. 561, spéc. pp. 593-596 (2001). – Laura QUILTER, Note, " The Continuing Expansion of Cyberspace Trespass to Chattels ", art. préc., spéc. pp. 437–433 (2002).

[1357] Dan L. BURK, " The Trouble with Trespass ", art. préc., spéc. p. 33 (2000).

[1358] Dan L. BURK, art. préc., spéc. pp. 35–37. – Laura QUILTER, art. préc., spéc. pp. 429-430 et pp. 439-441 (2002).

conséquences économiques pour ces derniers. Si l'on peut s'accorder sur le fait que la simple atteinte à la réputation du FAI ne peut constituer à elle seule le dommage exigé pour engager une action sur le fondement du *trespass to chattels*, elle participe néanmoins à l'évaluation du dommage. Par ailleurs, en considérant que seul le dommage direct (ou le risque de dommage) causé au système informatique puisse permettre d'engager la responsabilité du « spammeur », on pourrait aboutir à une situation paradoxale où l'engagement de sa responsabilité dépendrait moins du caractère illicite de l'activité que de l'incapacité du système informatique du FAI à absorber les effets néfastes des envois indésirables. En suivant ce raisonnement, il en résulterait que le propriétaire d'un équipement informatique doté d'un système techniquement plus fiable, serait juridiquement moins protégé que celui muni d'un dispositif de sécurité moins performant [1359]. À notre sens, cette position n'est pas soutenable et il convient de saluer la cour dans l'affaire *CompuServe* pour son pragmatisme dans la lutte contre ce fléau numérique qu'est le *spamming* en retenant une acception large de la notion de dommage.

C. LA QUESTION DU LIEN DE CAUSALITE EN MATIERE DE *SPAMMING*

460. L'appréciation théorique du lien de causalité. La preuve du lien de causalité, indispensable pour mettre en jeu la responsabilité délictuelle, se définit comme la relation de cause à effet entre le fait générateur et le dommage. Cette preuve est relativement aisée à rapporter lorsque le dommage résulte d'une cause unique. Or, le plus souvent, on constate qu'un dommage naît d'une multitude de causes. Dans cette circonstance, il convient alors de déterminer celles qui seront juridiquement considérées comme telles. Lorsque, par exemple, un internaute est confronté à un dysfonctionnement de sa messagerie, ce problème peut provenir d'une mauvaise configuration du logiciel de messagerie, d'une attaque par un virus, de la réception massive de *spams*, d'un matériel informatique obsolète ou encore d'une perturbation de son réseau ou de celui de son FAI. Parmi ces différentes causes, il conviendra de rechercher la ou les causes juridiques en rapport avec le dommage. Pour cela, deux méthodes sont envisageables. Selon la théorie dite de « la causalité adéquate », toutes les circonstances du dommage n'ont pas participé avec la même intensité à la réalisation du dommage. Est ainsi désignée comme cause juridique un évènement donné dès lors que, d'après le cours normal des choses, la faute rendait le dommage probable [1360]. Autrement dit,

[1359] V. ég. en ce sens, Patricia L. BELLIA, " Defending Cyberproperty ", art. préc., spéc. p. 2185 (2004).
[1360] Jacques FLOUR, Jean-Luc AUBERT, Éric SAVAUX, *Le fait juridique, op. cit.*, spéc. n° 167, pp. 193-194. – Philippe LE TOURNEAU, *Droit de la responsabilité et des contrats, op. cit.*, spéc. n° 1716, p. 567 et s. – Philippe MALAURIE, Laurent AYNES et Philippe STOFFEL-MUNCK, *Droit civil, Les obligations, op. cit.*, spéc. n° 93, p. 45

la cause doit être un antécédent nécessaire du dommage sans lequel le dommage ne se serait pas produit [1361]. En application de la théorie de « l'équivalence des conditions », sera qualifié de cause juridique tout évènement qui a participé nécessairement à la survenance du dommage. En d'autres termes, toute condition indispensable à la réalisation du dommage sera retenue comme causalité [1362]. En pratique, la mise en œuvre de ces théories se révèle difficile à manier et la complexité de la question relative à la détermination des causes du dommage rend délicate toute tentative de dégager les lignes directrices des solutions du droit positif. À cet égard, il est constaté qu' « [e]*n réalité les juridictions retiennent les deux théories : elles appliquent l'une ou l'autre au gré des espèces, en toute souplesse, d'une façon très favorable aux victimes. Il serait donc excessif d'affirmer que la théorie de la causalité adéquate est le plus souvent retenue. Tout au plus est-il possible de relever que l'équivalence des conditions est retenue de préférence dans la responsabilité subjective, tandis que la percée de la causalité adéquate est surtout produite dans les responsabilités*

(« *la théorie de la causalité adéquate cherche parmi les antécédents de l'accident le fait adéquat c'est-à-dire celui dont on peut considérer qu'il est la cause véritable. On estime qu'un évènement est la cause adéquate lorsqu'il est habituel qu'il le produise. La détermination de la cause adéquate appelle donc un diagnostic rétrospectif : en considérant le déroulement normal des choses tel que l'expérience le révèle, le fait reproché au défendeur rendait-il probable la réalisation du dommage ?* »). – Henri, Léon et Jean MAZEAUD, *Traité théorique et pratique de la responsabilité civile délictuelle et contractuelle*, tome 2, 6e éd., Montchrestien, 1970, spéc. n° 1441, p. 530 (« *celui qui a commis une faute doit réparer tout le préjudice qu'elle était propre à produire suivant le cours naturel des choses et qu'elle a effectivement produit* »).

[1361] La causalité a notamment été écartée lorsque s'intercale une circonstance causale qui n'a pas été provoquée ou été rendue nécessaire par le fait initial du défendeur, v. en ce sens, Cass. civ. 2e, 8 févr. 1989, *RTD civ.* 1989, p. 556 et s., obs. P. Jourdain (en l'espèce, victime d'un accident de la circulation, la personne en était restée handicapée et décéda dix ans plus tard à la suite des brûlures provoquées par l'incendie du lit sur lequel elle était étendue. La Cour de cassation ayant refusé de considérer comme les juges du fond que l'accident initial était une condition *sine qua non* du décès survenu, avait jugé que le décès avait pour cause immédiate l'incendie du lit. Selon les observations du professeur JOURDAIN, la Cour de cassation aurait raisonné en termes de causalité adéquate, et aurait ainsi considéré que le fait de l'automobiliste ne permettait pas de pronostiquer, selon le cours naturel des choses, ni l'incendie, ni moins encore le décès de la victime et le préjudice de la veuve. Il en conclut ainsi que « *le fait de l'auteur de l'accident initial ne serait pas tant écarté parce qu'il est une cause trop lointaine du dommage, que bien plutôt, parce qu'il n'en est pas la cause adéquate* » (note sous Cass. civ. 2e, 8 févr. 1989, arrêt préc., *RTD civ.* 1989, p. 556 et s.). – V. ég. Cass. civ. 2e, 13 juill. 2006, pourvoi n° 05-16645, *RTD civ.* 2007, p. 128, obs. P. Jourdain (« *il résulte des conclusions de l'expert que le nouveau préjudice résultait du nouvel accident survenu le 4 mars 1999, sans rapport avec celui de 1991 ; que la cour d'appel a pu en déduire que même si Mme X... avait un état prédisposant, conséquence du premier accident, elle n'avait subi aucune aggravation de son état antérieur* »). – Pour une étude approfondie et richement illustrée de ces différentes hypothèses, v. Patrice JOURDAIN, *Droit à réparation : Lien de causalité. – Détermination des causes du dommage, J.-Cl. Civil Code – Art. 1382 à 1386* , Fasc. 160, 2005, spéc. nos 20-32.

[1362] « *La cause est toute condition sine qua non du dommage* » (Jacques FLOUR, Jean-Luc AUBERT, Éric SAVAUX, *Le fait juridique, op. cit.*, spéc. n° 157, p. 182). – Philippe LE TOURNEAU, *Droit de la responsabilité et des contrats, op. cit.*, spéc. n° 1715, p. 656 et s. (observant que la théorie de l'équivalence des conditions est « *très favorable aux victimes* » puisque « *tous les éléments qui ont conditionné le dommage sont équivalents* »). – Pour une application de cette théorie, v. par ex. Cass. civ. 2e, 2 juin 2005, pourvoi n° 03-20.011, *Juris-Data* n° 2005-028683 ; *Bull. civ.* II, n° 146 ; *JCP* 2005, éd. G., IV. 2622 (en l'espèce, la concierge d'un immeuble avait omis de placer un sac poubelle, contenant des seringues jetées par un médecin exerçant dans l'immeuble, dans un bac spécialement conçu pour que les ordures ménagères soient enlevées sans autre manipulation que le bac lui-même. Un lien de causalité a été établi non seulement entre la faute de la concierge et le dommage subi par l'employé de service de ramassage des ordures qui s'est fait piqué par les seringues jetées sans précaution mais aussi entre les piqûres subies et la contamination de cet employé par le virus du VIH).

objectives dans lesquelles les rapports de causalité seront les plus complexes à déterminer » [1363].

461. L'appréciation du lien de causalité en droit positif et ses manifestations en cas de *spamming*. En droit positif, la causalité suppose que le fait générateur ait été nécessaire à la survenance du dommage allégué : « *L'exigence d'un rapport de nécessité entre le fait générateur et le dommage va naturellement conduire les juges à écarter le lien de causalité à chaque fois que l'évènement envisagé n'apparaît pas comme une condition sine qua non du dommage* » [1364]. En matière de *spamming*, il fait peu de doute que le « spammé » pourra établir aisément la preuve d'une relation causale entre la réception massive de *spams* et, selon le cas, l'encombrement de sa messagerie ou la saturation de son réseau, dès lors que ces conséquences découlent directement de l'activité d'un même « spammeur ». Il convient toutefois de préciser qu'il est possible d'identifier fréquemment la survenance successive de plusieurs dommages découlant d'un même fait générateur. Dans cette hypothèse, la question se pose de savoir si la personne responsable peut être tenue de réparer l'ensemble de ces dommages. La réponse à cette question est contenue dans l'article 1151 du Code civil relatif à la matière contractuelle disposant que « *les dommages-intérêts ne doivent comprendre* […] *que ce qui est la suite immédiate et directe de l'inexécution de la convention* ». Transposée en matière délictuelle [1365], le dommage réparable est ainsi limité à

[1363] Philippe LE TOURNEAU, *Droit de la responsabilité et des contrats, op. cit.*, spéc. n° 1717, p. 1718.

[1364] Geneviève VINEY et Patrice JOURDAIN, *Les conditions de la responsabilité, op. cit.*, spéc. n° 353, p. 197. – Pour des exemples de rejet d'actions en responsabilité, v. par ex. Cass. civ., 9 mars 1949, *JCP* 1949, éd. G., II. 4826 ; *D.* 1949, p. 331 et s. (a été rejetée l'existence d'un rapport de causalité entre la faute d'un expert exprimant un avis erroné dans un rapport et l'inculpation d'une personne dans la mesure où le juge ne s'est pas fondé sur ce rapport pour procéder à l'inculpation). – Cass. 2e civ., 7 févr. 1990, *Juris-Data* n° 1990-700371, pourvoi n° 86-17023 ; *Bull. civ.* II, n° 21 ; *RTD civ.* 1990, p. 487 et s., obs. P. Jourdain (refus de retenir un lien de causalité entre l'absence de port de la ceinture de sécurité et le dommage subi par le passager d'un véhicule à la suite d'un accident de la circulation en l'absence de « *relation de cause à effet entre les blessures constatées et l'absence du port de la ceinture de sécurité* »). – Cass. civ. 1re, 3 oct. 2000, *Juris-Data* n° 006126 ; *Resp. civ. assur.* janv. 2001, comm. 6, p. 13 (cassation de l'arrêt qui avait retenu la faute d'un pilote qui avait consisté à prendre un passager à bord, alors que cette faute n'avait pas de relation causale directe avec la chute de l'appareil ayant notamment entraîné le décès de l'un des passagers). – Cass. civ. 1re, 27 mai 2003, pourvoi n° 89-17.602 ; *Bull. civ.* I, n° 129 (retenant que le préjudice invoqué était dépourvu de lien de causalité avec la faute commise par un notaire). – Cass. civ. 3e, 12 juin 2003, *D.* 2004, p. 523, note S. Beaugendre (retenant l'absence de relation de cause à effet entre les faits reprochés au bailleur d'une maison de location de vacances concernant le non-bâchage d'une piscine d'une propriété dont il est le propriétaire et l'accident, la noyade d'un enfant). – Cass. civ. 2e, 20 nov. 2003, *Juris-Data* n° 2003-020895 ; pourvoi n° 01-17977 ; *Bull. civ.* II, n° 355 ; *D.* 2003, p. 2902 et s., concl. R. Kessous et note L. Grynbaum et 2004, somm., p. 1346, obs. D. Mazeaud ; *JCP* 2004, éd. G., I. 163, spéc. n° 36, obs. G. Viney ; *RTD civ.* 2004, p. 103 et s., obs. P. Jourdain (refus d'indemniser des dommages causés par l'usage du tabac en l'absence de lien de causalité entre le décès d'un fumeur et le prétendu comportement fautif de la SEITA). – Cass. civ. 1re, 9 mars 2004, pourvoi n° 01-17. 277 ; *Bull. civ.* I, n° 79 (rejet d'une demande d'indemnisation des parents pour le préjudice de leur enfant en l'absence de relation directe entre le handicap de leur enfant et la faute médicale commise).

[1365] Sur l'admission d'un mécanisme comparable en matière délictuelle, v. par ex. Muriel FABRE-MAGNAN, *Responsabilité civile et quasi-contrats, op. cit.*, spéc. p. 139. – V. ég. Geneviève VINEY et Patrice JOURDAIN, *Les conditions de la responsabilité, op. cit.*, spéc. n° 348, pp. 194-195 (« *Bien que visant expressément la seule responsabilité contractuelle, cette disposition est aujourd'hui unanimement considérée comme l'expression d'un principe applicable au domaine entier de la responsabilité civile* »).

celui qui est « *une suite immédiate tout au moins directe et suffisamment proche du fait générateur* » [1366]. *A priori*, l'application de cette disposition conduit à écarter tout dommage médiat et lointain par rapport au fait causal, ce dernier n'étant pas considéré comme étant à l'origine du dommage. Toutefois, l'analyse de la jurisprudence révèle que les juges n'hésitent pas à adopter, dans certaines hypothèses, une appréciation souple du lien de causalité pour admettre la réparation de dommages pourtant indirects [1367]. Ils ont notamment admis l'existence d'un lien de causalité entre un accident ayant entraîné un ralentissement de la circulation et la perte de recettes subie par une régie de transports urbains [1368] ou encore entre la chute des rochers d'une falaise et les préjudices commerciaux consécutifs à la décision municipale de fermeture d'un hôtel-restaurant situé en contrebas de la falaise pendant la durée des travaux de confortement [1369]. Cette appréciation souple du lien de causalité se vérifie également à la lecture de certaines décisions dans lesquelles les juges ont admis l'existence d'un lien de causalité lorsque le fait générateur a seulement aggravé le dommage et ce, alors même que sans lui, ce dernier se serait produit, mais de façon différente [1370]. La souplesse dont fait preuve la jurisprudence laisse penser qu'en matière de *spamming*, une entreprise qui serait victime d'un afflux massif de *spams*, à l'origine d'un ralentissement du traitement des *e-mails* de ses clients et qui subirait, par ricochet, la perte de clients insatisfaits par les services proposés ou encore une atteinte à sa réputation pourrait aussi obtenir la réparation de l'ensemble de ces dommages. De façon semblable, un FAI pourrait être indemnisé de la perte de certains de ses abonnés, perte consécutive à une saturation du

[1366] Muriel FABRE-MAGNAN, *Responsabilité civile et quasi-contrats*, *ibid.*, spéc. p. 139.

[1367] V. sur ce point, Jacques FLOUR, Jean-Luc AUBERT, Éric SAVAUX, *Le fait juridique*, *op. cit.*, spéc. n° 136, p. 154. – Geneviève VINEY et Patrice JOURDAIN, *Les conditions de la responsabilité*, *op. cit.*, spéc. n° 359, p. 207 et s. et les notes 94 et 95.

[1368] Cass. civ. 2, 28 avr. 1965, *D.* 1965, p. 777 et s., note P. Esmein (l'auteur d'une collision de véhicules ayant occasionné un encombrement est à bon droit condamné à réparer le préjudice subi par une régie de transports en commun dont les véhicules ont été retardés par cet encombrement, retard qui a entraîné pour cette régie une diminution de recettes).

[1369] Cass. civ. 2e, 26 sept. 2002, pourvoi n° 00-18627 ; *Juris-Data* n° 2002-015653 ; *Bull. civ.* II, n° 198 ; *Resp. civ. assur.* déc. 2002, comm. 351, p. 14 ; *RTD civ.* 2003, p. 100 et s., obs. P. Jourdain (« *l'arrêté municipal ne trouvait lui-même sa justification qu'au regard du risque d'éboulement de la falaise, n'en étant que la conséquence, et que ce risque constituait donc la cause de la cessation d'exploitation de l'établissement* »).

[1370] Geneviève VINEY et Patrice JOURDAIN, *Les conditions de la responsabilité*, *op. cit.*, spéc. n° 353-1, p. 198. – Pour des cas limites où la causalité a été admise, v. par ex. Cass. civ. 2e, 23 avr. 1969, *Bull. civ.* II, n° 132 ; *D.* 1969, p. 562; *JCP* 1969, éd. G., II. 1596 (il a été jugé que même si la faute d'imprudence de la victime n'a pas de lien de causalité avec l'accident dont elle est victime, cette faute ayant concouru à l'aggravation du dommage corporel subi doit entraîner l'exonération partielle du conducteur responsable). – Cass. civ. 1re, 16 juin 1969, *Bull. civ.* I, n° 184 ; *D.* 1969, p. 586 ; *JCP* 1970, éd. G., II. 16412, note R. Savatier (en l'espèce, la victime blessée par une voiture de X, la compagnie d'assurance de X avait demandé à la victime de se faire examiner par son médecin-conseil ; que celui-ci avait demandé à un spécialiste de pratiquer une aérographie qui entraîna sa mort. Selon le pourvoi, le décès lié à cet examen n'avait pas de rapport direct avec l'accident proprement dit et ne devait pas être pris en charge, la victime légèrement blessée avait repris le travail et s'était librement soumise à cet examen : « *ayant constaté que* [la victime d'un] *accident dont étaient responsables* [des personnes garanties par une compagnie d'assurance], *ne s'était rendue chez* [un docteur], *qui pratiqua l'artériographie*, [à la suite de laquelle est survenu le décès], *qu'à la demande du médecin-conseil de la compagnie* [d'assurance], *et pour les besoins de l'examen, et que le praticien n'avait commis aucune faute, la cour d'appel a pu déclarer, sans dénaturation que le décès* [de la victime] *était en relation de cause à effet avec l'accident dont* [elle] *a été victime* »).

réseau et/ou l'encombrement de sa bande passante engendrée par la réception très importante de *spams*, l'empêchant ainsi de proposer un fonctionnement optimal de ses services. La reconnaissance d'un préjudice économique réparable semble plaider en ce sens.

D. LA QUESTION DE LA REPARATION DES « SPAMMES »

462. Une fois que la victime est parvenue à prouver l'existence d'un lien de causalité entre le fait générateur et le dommage éprouvé [1371], la personne poursuivie est donc déclarée responsable du dommage subi et est tenue de le réparer. Cette obligation de réparation est guidée par le principe de la réparation intégrale (1.). Après en avoir exposé les modalités, il conviendra d'évaluer si la réparation obtenue sur le fondement de l'article 1382 du Code civil serait satisfaisante au regard des dommages éprouvés par les « spammés » (2.).

1. Le principe de réparation intégrale

463. Le principe. Le principe est celui d'une réparation intégrale du dommage subi par la victime qui consiste à « rétablir aussi exactement que possible l'équilibre détruit par le dommage et de replacer aussi exactement que possible la victime, aux dépens du responsable, dans la situation où elle se serait trouvée si l'acte dommageable n'avait pas eu lieu » [1372]. En vertu de ce principe, la victime doit obtenir réparation de « tout le préjudice et rien que le préjudice » [1373] sans distinction entre des chefs de préjudice [1374], étant précisé

[1371] La charge de la preuve du lien de causalité incombant à la victime du dommage. – V. par ex. Geneviève VINEY et Patrice JOURDAIN, *Les conditions de la responsabilité*, *op. cit.*, spéc. n° 361 et s., p. 210 et s. – François TERRE, Philippe SIMLER et Yves LEQUETTE, *Les obligations*, *op. cit.*, spéc. n° 861, p. 867.

[1372] Cass. civ. 2e, 28 oct. 1954, *Bull. civ.* II, n° 328 ; *RTD civ.* 1955, p. 324, spéc. n° 34, obs. H. et L. Mazeaud ; *JCP* 1955, éd. G., II. 8765, note R. Savatier. – Se prononçant dans des termes similaires, v. Cass. civ. 2e , 1er avr. 1963, *D.* 1963, p. 453, note H. Molinier ; *JCP* 1963, II. 13408, note P. Esmein. – Cass. civ. 2e, 18 janv. 1973, *JCP* 1973, II. 17545, note M. A ; *RTD civ.* 1974, p. 159, obs. G. Durry. – Cass. civ. 2e, 4 févr. 1982, *inédit*, pourvoi n° 80-17139 ; *JCP* 1982, éd. G., II. 1984, note J.-F. Barbieri ; *Gaz. Pal.*1983, pan., p. 355, note F. Chabas. – Il a également été jugé que « *si la réparation d'un dommage ne peut excéder le montant du préjudice, elle doit, en tout cas, être intégrale* » (v. Cass. civ. 2e, 6 juill. 1983, pourvoi n° 82-10581; *Bull. civ.* II, n° 143).

[1373] François TERRE, Philippe SIMLER et Yves LEQUETTE, *Les obligations*, *op. cit.*, spéc. nos 899-900, pp. 913-914. – Pour une étude approfondie de ce principe, v. Christelle COUTANT-LAPALUS, *Le principe de la réparation intégrale en droit privé*, (préf. Frédéric POLLAUD-DULIAN), P.U.A.M., 2002, spéc. n° 4, p. 20 et la note 10 (« *la réparation de tout le préjudice et uniquement de ce préjudice* »). – V. ég. Philippe LE TOURNEAU, *Droit de la responsabilité et des contrats*, *op. cit.*, spéc. nos 2521-2546, pp. 796-806. – Muriel FABRE-MAGNAN, *Responsabilité civile et quasi-contrats*, *op. cit.*, spéc. pp. 372-377 (le responsable doit compenser tous les préjudices subis par la victime : celui causé directement par le dommage mais aussi ceux qui en sont une conséquence directe. Ainsi, le dommage n'est pas limité à celui que l'auteur pourrait prévoir mais il est tenu de « *réparer tous les dommages effectivement survenus, même s'ils dépassent ceux que l'on pouvait raisonnablement prévoir* » (*id.*, p. 372)).

[1374] Cass. crim., 16 janv. 1980, pourvoi n° 79-91793, arrêt préc. (« *si les juges du fond apprécient souverainement le préjudice dans la limite des conclusions des parties, ils doivent tenir compte de tous les chefs*

qu'elle doit s'effectuer « sans perte ni profit pour la victime » [1375]. Cette règle permet non seulement de remettre la victime dans sa situation initiale avant la survenance du dommage mais l'autorise aussi à demander l'indemnisation des frais induits par ce dommage [1376]. Par ailleurs, rappelons que la gravité de la faute doit rester sans influence sur le montant des dommages-intérêts car le juge qui condamne le responsable ne le frappe pas d'une peine, mais l'oblige à réparer un dommage [1377]. En effet, qu'il s'agisse d'une faute lourde, d'une faute légère d'imprudence ou de négligence, « il n'y a, pour la réparation, que le résultat qui compte » [1378]. S'agissant de l'étendue du dommage matériel réparable, l'article 1149 du Code civil relatif à la responsabilité contractuelle, et étendu au domaine délictuel [1379],

de dommage, aussi bien matériels que corporels ou moraux découlant des faits, objets de la poursuite, pour en réparer l'intégralité »). – Henri et Léon MAZEAUD, Jean MAZEAUD et François CHABAS, *Traité théorique et pratique de la responsabilité civile délictuelle et contractuelle*, (préf. Henri CAPITANT), tome 3, vol. 1, 6e éd., Montchrétien, 1978, spéc. n° 2364. – Pour une critique de la généralité de l'article 1382 du Code civil, v. Geneviève VINEY dénonçant « *la totale méconnaissance de la hiérarchie des intérêts à protéger* » et estimant que cette disposition « *ne fait aucune différence entre les préjudices, le concept de dommage étant unique et indifférencié* » (« Pour ou contre un " principe général " de responsabilité pour faute ? : Une question posée à propos de l'harmonisation des droits civils européens » *in Le droit privé français à la fin du XXe siècle, Études offertes à Pierre CATALA*, Litec, coll. *Les Traités*, 2001, p. 555 et s., spéc. n° 12, p. 563) ; *Introduction à la responsabilité*, 3e éd., L.G.D.J., coll. *Traité de droit civil*, 2008, spéc. n° 65 ; v. ég. antérieurement note sous Cass. civ. 2e, 27 mai 1999, *JCP* 2000, éd. G., I. 197, spéc. n° 6 (« *la responsabilité n'est pas fait pour réparer intégralement tous les dommages imaginables, mais pour répondre à une demande sociale de compensation qui est plus ou moins impérieuse et plus ou moins légitime selon la nature de l'intérêt atteint et la gravité du préjudice. Nier cette gradation des attentes sociales n'est ni juste ni réaliste, du point de vue économique* »). – Rappr. Jean-Sébastien BORGHETTI, « Les intérêts protégés et l'étendue des préjudices réparables en droit de la responsabilité civile extra-contractuelle », art. préc.., spéc. pp. 166 et s. (proposant pour sa part « *une protection différenciée des intérêts* » : « *Il ne s'agit pas de remettre en cause ce principe général – mais non absolu ! – du droit français* […]. *Il convient cependant de lui donner sa juste place. L'article 1382 n'affirme pas, en effet, que tout dommage doit être réparé, quel que soit le fondement de la responsabilité. Dès lors, il est tout à fait possible, sans contrevenir à la lettre ni même sans doute à l'esprit de ce texte fondateur, d'estimer qu'en cas de responsabilité reposant sur un autre fondement que la faute, les préjudices résultant d'atteinte aux biens corporels ou à des intérêts incorporels ne sont pas réparables qu'en tant que leur réparation correspond à la ratio legis du régime de responsabilité invoqué* » (*idem*, spéc. p. 170)).

[1375] V. par ex. Cass. crim., 21 oct. 1998, pourvoi n° 97-84.414, *inédit* (« *le calcul du préjudice doit être fait de manière qu'il n'en résulte pour la victime ou ses ayants droit ni perte, ni profit* »). – Cass. civ. 2e, 23 janv. 2003, pourvoi n° 01-00.200, *Bull. civ.* II, n° 20 ; *JCP* 2003, éd. G., II. 10110, note J.-F. Barbieri ; *D.* 2005, I.R., p. 605 (« *les dommages-intérêts alloués à une victime doivent réparer le préjudice subi sans qu'il en résulte pour elle ni perte ni profit* »). – Cass. civ. 1re, 9 nov. 2004, pourvoi n° 02-12.506, *Bull. civ.* I, n° 264, p. 220 (la Cour a jugé que « *la réparation d'un dommage, qui doit être intégrale, ne peut excéder le montant du préjudice* ». A ainsi violé l'article 1382 du Code civil une cour d'appel qui a évalué le préjudice sans prendre en compte l'avantage au profit des possesseurs de bonne foi que représentait « *la conservation des fruits et des revenus, en dépit de l'effet rétroactif de l'annulation de la vente* »). – Cass. civ. 3e, 8 juill. 2009, pourvoi n° 08-10869, *Bull. civ.* III, n° 170. – Cass. civ. 1re, 25 mars 2009, pourvoi n° 07-20774 ; *Bull. civ.* I, n° 70. – Le principe de réparation intégrale est réaffirmé dans le projet CATALA : « *Sous réserve de dispositions ou de conventions contraires, l'allocation de dommages-intérêts doit avoir pour objet de replacer la victime autant qu'il est possible dans la situation où elle se serait trouvée si le fait dommageable n'avait pas eu lieu. Il ne doit en résulter pour elle ni perte ni profit* » (proposition d'article 1370 du C. civ.).

[1376] Cass. civ. 1re, 1er juill. 1997, pourvoi n° 95-16.771, *Bull. civ.* I, n° 225 (une société concessionnaire de l'exploitation d'une autoroute est en droit d'obtenir de l'auteur de l'accident l'indemnisation intégrale de son préjudice, y compris les frais exposés pour la protection et la surveillance des lieux de l'accident).

[1377] Henri, Léon et Jean MAZEAUD et François CHABAS, *Leçons de droit civil, Les obligations, op. cit.*, spéc. n° 623, p. 735. – Pour une étude approfondie sur l'influence de la gravité de la faute et la prise en compte de ce caractère dans certaines hypothèses, v. Geneviève VINEY et Patrice JOURDAIN, *Les conditions de la responsabilité, op. cit.*, spéc. n° 595 et s., p. 616 et s., et en particulier n° 599, p. 620.

[1378] Henri et Léon MAZEAUD, Jean MAZEAUD et François CHABAS, *Traité théorique et pratique de la responsabilité civile délictuelle et contractuelle*, 1978, *op. cit.*, spéc. n° 2364, p. 717.

[1379] Yvaine BUFFELAN-LANORE et Virginie LARRIBAU-TERNEYRE, *Droit civil : Les obligations, op. cit.*, spéc. n° 1599, p. 538.

dispose que : « [l]*es dommages et intérêts dus au créancier sont, en général, de la perte qu'il a faite et du gain dont il a été privé* ». En cas d'accident de voiture, par exemple, on tiendra compte des dégâts effectifs du véhicule, des frais de réparation auxquels peut s'ajouter une indemnité destinée à compenser la perte de jouissance du véhicule pendant la durée de la réparation. Au regard de cette indemnisation particulièrement large, la réparation à laquelle pourrait prétendre le « spammé » pourrait couvrir non seulement les frais liés à l'acquisition de logiciel de sécurité [1380], ceux provenant de l'achat de bande passante supplémentaire, mais également ceux engagés pour recourir à un service de spécialistes en informatique. Enfin, lorsqu'il est question de la réparation du dommage moral, le principe de la réparation intégrale semble toutefois en net recul puisque celle-ci s'analyse généralement comme une peine privée, définie comme « une sanction civile punitive indépendante de toute idée réparatrice, infligée à l'auteur d'une faute qui lui est moralement imputable, au profit exclusif de la victime qui peut, seule, en demander l'application » [1381].

464. Les modalités de la réparation. La réparation du dommage peut s'effectuer selon deux procédés dont le choix revient aux juges du fond qui bénéficient d'un pouvoir souverain en la matière [1382]. La réparation peut donc être réalisée sous la forme d'une réparation en nature ou d'une réparation par équivalent. S'agissant de la réparation en nature [1383], cette dernière consiste « *à rétablir, strictement, l'état de chose antérieur au dommage en procurant à la victime ce dont elle a été strictement privée* […] *le dommage se trouve alors radicalement effacé* » [1384]. Concrètement, en cas de dommage matériel, les juges peuvent ainsi condamner l'auteur du dommage à « *remettre en l'état le bien qu'il a détérioré, de remplacer ce qu'il a détruit, de mettre fin à l'état de choses irrégulier qu'il avait créé* » [1385]. Cette large réparation lui vaut ainsi d'être reconnue comme « *le mode de*

[1380] V. en ce sens, TGI Paris, réf., 26 mai 2003, *SNES* c/ *La Droite Libre et al.*, jugement préc. (les juges ayant accordé une réparation au titre de l'achat d'un logiciel anti-*spam* permettant de stopper les troubles engendrés par l'afflux de très nombreux messages).

[1381] Alexis JAULT, *La notion de peine privée*, (sous la dir. de François CHABAS), tome 442, L.G.D.J., coll. *Bibl. dr. privé*, 2005, spéc. n° 415, p. 273 (l'auteur ajoute que « *la peine privée s'analyse en une sanction punitive destinée à garantir l'ordre juridique privé, c'est-à-dire les intérêts de la victime de l'acte illicite sanctionné* » (*id.*, spéc. n° 141, p. 271). – Sur la tendance jurisprudentielle à alourdir le montant des dommages et intérêts en cas de préjudice moral ou de faute lucrative, v. *infra :* n° 475).

[1382] Théodore IVAINER, « Le pouvoir souverain du juge dans l'appréciation des indemnités réparatrices », *D.* 1972, chron., p. 3 et s. – L'article 1368 du projet de réforme du droit des obligations consacre expressément le choix pour le juge, de réparer en nature ou sous la forme de dommages et intérêts, tout en précisant que les deux types de mesure peuvent se cumuler pour assurer la réparation intégrale du préjudice.

[1383] V. Projet CATALA précité qui consacre expressément cette forme de réparation (v. proposition d'articles 1369 et 1369-1 du C. civ.). – V. ég. proposition de loi de 2010 préc., spéc. proposition d'article 1386-22 du C. civil.

[1384] Jacques FLOUR, Jean-Luc AUBERT, Éric SAVAUX, *Le fait juridique, op. cit.*, spéc. n° 385, p. 472. – V. ég. proposition de loi de 2010 préc., spéc. proposition d'article 1386-22 du C. civ. : « *La réparation en nature du dommage a pour objet de supprimer, réduire ou compenser le dommage* ».

[1385] Jacques FLOUR, Jean-Luc AUBERT, Éric SAVAUX, *ibid.*, spéc. n° 385, p. 472.

réparation le plus parfait » [1386]. Par ailleurs, il convient de préciser que si le responsable offre la possibilité de réparer en nature le dommage subi, la victime ne peut le refuser sous réserve que cette réparation ne présente pas pour cette dernière un danger ou un inconvénient [1387]. En revanche, dans le cas où le responsable ne propose pas de réparation en nature, la victime est libre de la demander ou non sans que le juge ne soit toutefois tenu de l'ordonner [1388]. Dans bien des hypothèses, la réparation en nature sera néanmoins difficilement concevable, en particulier lorsque la victime subit un préjudice moral. Dans ce cas, la victime devra se contenter d'une réparation par équivalent. Cette seconde modalité de réparation consiste le plus souvent en un versement de dommages et intérêts [1389], la somme allouée à la victime venant compenser, par une valeur équivalente, la perte éprouvée (on parle ainsi de « dommages et intérêts compensatoires »). Le montant de la réparation est déterminé en considération du préjudice subi sans prendre en compte la gravité de la faute commise [1390]. L'évaluation du préjudice est laissée à l'appréciation des juges du fond [1391]. Dans un arrêt du 26 mars 1999, l'Assemblée plénière de la Cour de cassation dispense explicitement les juges du fond de toute motivation quant à l'évaluation du dommage : « *attendu que la cour d'appel a apprécié souverainement le montant du préjudice dont elle a justifié l'existence par l'évaluation qu'elle en a fait, sans être tenue d'en préciser les divers éléments* » [1392]. Les juges du fond doivent seulement réparer tous les chefs de préjudice [1393] ;

[1386] Henri, Léon et Jean MAZEAUD et François CHABAS, *Leçons de droit civil, Les obligations : théorie générale, op. cit.*, spéc. n° 621, p. 732.
[1387] Henri, Léon et Jean MAZEAUD et François CHABAS, *ibid.*, spéc. n° 621, pp. 732-733.
[1388] Henri, Léon et Jean MAZEAUD et François CHABAS, *ib.*, spéc. n° 621, p. 733.
[1389] Il peut également s'agir d'une réparation par équivalent non pécuniaire. Tel est le cas par exemple de la publication du jugement condamnant le responsable, le juge étant libre de l'ordonner (en ce sens, v. Cass. com. 5 déc. 1989, pourvoi n° 87-15309, *Bull. civ.* IV, n° 307 ; *D.* 1990, I.R., p. 14). – Sur la relation entre l'indemnité, la réparation et le principe de la réparation intégrale, v. Cécile LE GALLOU, *La notion d'indemnité en droit privé,* (préf. Alain SERIAUX), L.G.D.J., coll. *Bibl. dr. privé,* 2007, spéc. n° 111 et s., p. 106 et s. (« *La responsabilité civile, qui poursuit l'objectif de retour au statu quo ante, exprimé par l'article 1382 du Code civil, illustre l'application de la notion d'indemnité. En effet, les pertes provoquées par les délits ou les quasi-délits ne sont pas voulues par la victime ; ni dans leur réalisation, ni au moment de leurs effets : l'appauvri subit une perte et il ne consent pas à ce que le déséquilibre ainsi créé perdure. Face à un appauvrissement sans cause provoqué par un tiers, la responsabilité civile organise la suppression du déséquilibre par le versement de l'indemnité* »). – V. ég. proposition de loi de 2010 préc., spéc. proposition d'article 1386-24 du C. civil.
[1390] V. par ex. Cass. civ. 2e, 8 mai 1964, *JCP* 1965, éd. G., II. 14140, note P. Esmein ; *RTD civ.* 1965, n° 20, p. 137, obs. R. Rodière (« *L'indemnité nécessaire pour compenser le préjudice subi doit être calculée en fonction de la valeur du dommage, sans que la gravité de la faute puisse avoir aucune influence sur le montant de la dite indemnité* »).
[1391] V. not. Théodore IVAINER, « Le pouvoir souverain du juge dans l'appréciation des indemnités réparatrices », chron. préc. – V. par ex. Civ 1re, 16 juill. 1991, pourvoi n° 90-10.843, *Bull. civ.* I, n° 249 ; *JCP* 1991, éd. G., IV. 367 ; *JCP* 1992, éd. G., I. 3572, obs. G. Viney (« *L'existence et l'étendue du préjudice relevant de l'appréciation des juges du fond ; qu'en énonçant que la somme allouée par elle constituait réparation de tous les préjudices invoqués par* [la demanderesse], *la cour d'appel qui n'était pas tenue de s'expliquer sur chacun des préjudices, a nécessairement considéré que les fautes qu'elle avait retenues* […] *trouvaient ainsi leur réparation* »).
[1392] Cass. Ass. plén., 26 mars 1999, pourvoi n° 95-20640 ; *Juris-Data* n° 001247 ; *Bull. Ass. plén.*, n° 3, p. 3 ; *JCP* 2000, éd. G., I. 199, spéc. n° 12, note G. Viney.
[1393] V. par ex. Cass. crim. 16 janv. 1980, pourvoi n° 79-91793, arrêt préc. (« *si les juges du fond apprécient souverainement le préjudice dans la limite des conclusions des parties, ils doivent tenir compte de tous les chefs de dommage, aussi bien matériels que corporels ou moraux découlant des faits, objet de la poursuite, pour en réparer l'intégralité* »).

toute réparation forfaitaire est exclue [1394]. La mise en œuvre de ce principe offre donc une certaine souplesse par rapport aux indemnités plafonnées puisque le montant de la réparation est adapté à la diversité des préjudices constatés. Toutefois, comme le souligne à juste titre le professeur Geneviève VINEY, l'appréciation souveraine des juges du fond quant au préjudice « *consacre, dans un domaine très important, une renonciation pure et simple de la Cour de cassation à assurer deux missions essentielles de contrôle de l'application du droit par les juges du fond et d'unification de son interprétation sur l'ensemble du territoire. Or cette mission est, de toute évidence, préjudiciable tant aux plaideurs eux-mêmes qu'à la cohérence et à la qualité du système français de responsabilité civile* » [1395]. Dans cette lignée, le projet CATALA s'oppose à l'évaluation globale du préjudice posée par la Cour de cassation : « *Le juge doit évaluer distinctement chacun des chefs de préjudice allégués qu'il prend en compte. En cas de rejet d'une demande relative à un chef de préjudice, le juge doit motiver spécialement sa décision* » [1396]. De même, la proposition de loi de 2010 suggère l'insertion d'un nouvel article 1386-27 dans le Code civil qui poserait le principe de l'évaluation distincte des chefs de préjudice par le juge : « *À l'exception des dommages inférieurs au taux de compétence du juge de proximité, le juge évalue distinctement chacun des chefs de préjudice allégués qu'il prend en compte* ».

465. L'évaluation de la perte de chance. Si le principe de l'indemnisation de la perte de chance est admis [1397], se pose dès lors la question de son mode de calcul [1398]. Rappelons au préalable que la chance correspond à la probabilité que l'évènement escompté se réalise et que le dommage résulte de la disparition de cette chance. Il ne s'agit donc pas d'indemniser l'avantage espéré qui, par hypothèse, ne se réalisera pas, mais la perte d'une chance sérieuse. La réparation de cette perte de chance sera nécessairement partielle. La Cour de cassation a clairement rappelé ce principe de l'indemnisation dans un arrêt récent : « *la réparation d'une perte de chance perdue doit être mesurée à la chance perdue et ne peut être égale à l'avantage qu'aurait procuré cette chance si elle s'était réalisée* » [1399]. À cet

[1394] Cass. civ. 3e, 3 juin 2004, pourvoi n° 03-11.475 ; *Juris-Data* n° 2004-023963 ; *Resp. civ. assur.* sept. 2004, comm. 256, p. 22 (a été cassé l'arrêt de la cour d'appel qui avait fixé le préjudice à une somme forfaitaire alors que la victime devait être replacée dans la situation où elle se serait trouvée si l'acte dommageable ne s'était pas réalisé). – V. déjà en ce sens, Cass. civ. 1re, 2 avr. 1996, pourvoi n° 94-13.871; *Bull. civ*. I, n° 166 ; 3 juill. 1996, pourvoi n° 94-14.820, *Bull. civ*. I, n° 296 ; *D.* 1996, I.R., p. 194.

[1395] Geneviève VINEY, note sous Cass. Ass. plén., 26 mars 1999, arrêt préc., *JCP* 2000, éd. G., I. 199.

[1396] Projet CATALA préc., art. 1374.

[1397] V. *supra* : n° 454.

[1398] Sur cette question, v. Caroline RUELLAN, « La perte de chance en droit privé », art. préc., spéc. n° 48, pp. 751-752. – V. not. Geneviève VINEY et Patrice JOURDAIN, *Les conditions de la responsabilité*, *op. cit*., spéc. no 277 et s., p. 89 et s.

[1399] Cass. civ. 2e, 9 avr. 2009, arrêt préc., *JCP* 2009, éd. G., IV. 1831 ; *LPA* 23 juill. 2009, n° 146, p. 18 et s., note A. Dumery (cassation de l'arrêt d'appel qui avait admis que l'étudiant ayant perdu deux ans de scolarité en raison des séquelles d'un accident avait subi la perte d'une chance d'avoir un emploi de cadre et l'avait indemnisé en considérant que « *la perte de chance subie peut être équivalente à la différence de revenus entre*

égard, la proposition de loi de 2010 suggère que l'article 1384 du Code civil soit ainsi rédigé : « *La perte d'une chance constitue un préjudice réparable distinct de l'avantage qu'aurait procuré cette chance si elle s'était réalisée* » [1400]. Le montant de l'indemnité sera ainsi calculé en fonction de la probabilité qu'il y aurait eu d'obtenir le succès si la faute n'avait pas empêché sa réalisation [1401]. Cette réparation partielle s'explique par le fait que lorsque la chance est constitutive d'un préjudice, il existe en réalité deux préjudices distincts : le préjudice final futur, par essence, éventuel et le « *préjudice intermédiaire, constitué par la disparition de la situation en devenir,* [qui] *est saisi par le droit à travers la qualification de perte de chance* [1402]. Le calcul de la perte d'une chance résulte ainsi d'une double évaluation : l'évaluation du gain si la chance s'était pleinement réalisée et celle de la chance elle-même qui constitue une fraction du préjudice final [1403]. Si la perte de chance et le préjudice final sont autonomes dans leur existence, l'évaluation de la perte de chance est

ceux d'un cadre supérieur et ceux d'un employé, équivalent à un SMIC ». La Cour de Cassation a donc jugé qu'« *en tenant pour acquis que la victime aurait obtenu un poste de cadre supérieur et en indemnisant la perte de salaire correspondante capitalisée, la cour d'appel a violé l'article 1382 du Code civil* »). – v. ég. Cass, civ. 1re, 16 juill. 1998, pourvoi n° 96-15380, *Bull. civ.* I, n° 260. –Dans un contexte similaire, v. ég. Cass. civ. 2e, 27 févr. 1985, *Bull. civ.* II, n° 52 ; *RTD* civ. 1986, p. 117, obs. J. Huet (indemnisation d'accidenté de la circulation pour la « *perte d'une chance d'obtenir un meilleur emploi* » en raison des séquelles de l'accident mais sans prendre en compte la rémunération afférant à un poste de gérant agricole que la victime souhaitait assurer, faute d'avoir démontré qu'elle aurait pu l'obtenir aux conditions souhaitées). – Cass. civ. 1re, 9 avr. 2002, pourvoi n° 00-13.314 ; *Juris-Data* n° 2002-013914 ; *Bull. civ.* I, n° 116.

[1400] Proposition de loi portant réforme de la responsabilité civile, proposition préc. – V. déjà en ce sens le projet Catala préc., l'art. 1346 posait une rédaction identique.

[1401] V. not. Alain BENABANT, *Les obligations*, *op. cit.*, spéc. n° 679, p. 485. – Jacques FLOUR, Jean-Luc AUBERT, Éric SAVAUX, *Le fait juridique*, *op. cit.*, spéc. n° 138, p. 158 (le montant de la réparation « *correspondra à un certain pourcentage – établi par le calcul de probabilité – de l'indemnité que le dommage effectivement subi aurait justifié s'il n'y avait pas eu simple perte chance* »). […] « *En bref, celui qui ne peut justifier d'une chance perdue, donc d'une simple probabilité d'obtenir un gain, ou d'éviter une perte, ne peut se prévaloir que de cette perte de chance : il ne saurait réclamer une indemnité égale à la totalité du gain manqué ou de la perte subie* » (*idem.*, spéc. n° 138, p. 159).– Philippe MALAURIE, Laurent AYNES et Philippe STOFFEL-MUNCK, *Les obligations*, *op. cit.*, spéc. n° 242, pp. 135-136 (« *Lorsque la perte de chance est réparable les dommages et intérêts alloués à la victime ne sont qu'une fraction de l'avantage espéré, plus ou moins forte selon la probabilité. L'indemnité n'est donc pas égale à la totalité du gain espéré, dont l'obtention par hypothèse est aléatoire. De redoutables problèmes de probabilités se posent donc que la jurisprudence résout de manière radicale en posant en principe que l'évaluation faite par les juges du fond est souveraine* »). – Caroline RUELLAN, précisant en outre que « *Le dommage étant distinct, la réparation est celle d'une espérance perdue. Elle est totale au regard de ce que la victime a subi comme dommage, bien qu'elle consiste en une somme moindre que celle qui aurait été octroyée si l'évènement escompté se fût produit. Il ne saurait être question d'accorder à la victime la totalité de l'avantage espéré* » (« La perte de chance en droit privé », art. préc., spéc. n° 48, p. 752).

[1402] Caroline RUELLAN, « La perte de chance en droit privé », art. préc., spéc. n° 24, p. 740 (« *Ce préjudice est spécial car il s'analyse en la perte d'une probabilité, autonome par rapport au préjudice final* »). – De même, le projet CATALA la définit comme « *la perte de chance constitue un préjudice réparable distinct de l'avantage qu'aurait procuré cette chance si elle s'était réalisée* » (art. 1346). – *Contra* Jacques BORE qui considère que « [l]*e dommage résultant de la perte d'une chance n'est donc pas distinct du dommage final, si ce n'est sur le plan d'une appréciation purement causale* » (« L'indemnisation pour les chances perdues : une forme d'appréciation quantitative de la causalité d'un fait dommageable », chron. préc., spéc. n° 13). – Sur ce préjudice intermédiaire : v. Henri et Léon MAZEAUD et André TUNC, *Traité théorique et pratique de la responsabilité civile délictuelle et contractuelle*, *op. cit*, spéc. n° 219, p. 273 et s. (« *c'est la valeur de cette chance, ou de chances semblables, que les tribunaux devront s'efforcer d'évaluer* » (*id.*, spéc. n° 219, p. 278).

[1403] Cass. civ. 1re, 8 juill. 1997, *Bull. civ.* I, nos 238 et 239 ; 18 juill. 2000, *Bull. civ.* I, n° 224 ; *D.* 2000, p. 853, note Y. Chartier ; 18 janv. 2005, *Bull. civ.* I, n° 29.

donc nécessairement liée à celle du préjudice final [1404], de sorte que toute modification affectant l'évaluation du préjudice final entraîne automatiquement une aggravation du préjudice constitué par la perte de chance [1405]. En définitive, « [l]*a somme réparant la perte de chance tendra d'autant plus vers le montant de la réparation du dommage final que la chance réelle et sérieuse était grande, que la probabilité était élevée* » [1406].

466. Indifférence quant à la négligence de la victime. Si le montant de la réparation peut être étendu, en revanche, peut-il être réduit en raison de la négligence de la victime qui aurait ainsi contribué à la réalisation de son propre dommage ? La négligence constitue une faute légère, visée par l'article 1383 du Code civil. Comme toute faute, elle devrait conduire, lorsqu'elle émane de la victime, à un partage de responsabilité. Telle est la question qui se pose précisément dans le cas où un « spammé » aurait, de façon indirecte, concouru à la survenance de son propre dommage en faisant preuve d'inertie, en s'abstenant, par exemple, de s'équiper de mesures élémentaires de filtrage ou en commettant une erreur de manipulation de son logiciel anti-*spam*. Les juges se sont clairement prononcés par la négative en rejetant l'argument selon lequel le demandeur aurait pu se prémunir contre la réception de *spams* grâce à la mise en place d'une « *installation logicielle simple* », installation qui aurait permis de limiter son préjudice [1407]. Cette solution s'inscrit dans le droit fil de la position de la chambre criminelle de la Cour de cassation qui s'oppose fermement à ce qu'une simple négligence de la victime puisse justifier une diminution du montant de l'indemnisation que doit lui verser l'auteur d'une infraction intentionnelle contre les biens [1408]. Cette solution apparaît donc protectrice de la victime, et fait écho au rejet par la jurisprudence d'une solution qui conduit à soumettre la victime à une obligation de

[1404] Comme l'explique très clairement Philippe JOURDAIN, « *la perte de chance est un préjudice spécifique et autonome en ce sens qu'il ne doit pas être confondu avec le préjudice final et ne constitue pas une fraction de celui-ci. Mais l'évaluation de la perte de chances d'éviter un dommage est nécessairement fonction de ce dommage* [final] *; l'indemnité qui la répare s'obtient par l'application à la valeur du dommage final d'un pourcentage représentant ces chances. Si le dommage final varie après une première évaluation, la perte de chance doit donc varier dans la même proportion* » (obs. sous Cass. civ. 1re, 7 juin 1989, *RTD* civ. 1992, spéc. pp. 113-114).

[1405] Cass. civ. 1re, 7 juin 1989, arrêt préc. (la perte de chance qui constitue un préjudice « *est fonction de la gravité de l'état réel de la victime de sorte que l'étendue du dommage pourrait se trouver modifiée par l'aggravation de son incapacité* »). – V. ég. CA Paris, 4 juill. 1977, *JCP* 1997, éd. G., II. 1978, note G. Flécheux (« *la perte d'une chance aussi importante constitue un dommage qui ne saurait être équitablement apprécié sans référence à l'étendue du préjudice réellement subi* »).

[1406] Caroline RUELLAN, « La perte de chance en droit privé », art. préc., spéc. n° 49, pp. 752-753.

[1407] TGI Paris, réf., 26 mai 2003, *SNES* c/ *La Droite Libre et al.*, jugement préc.

[1408] La chambre criminelle de la Cour de cassation juge très régulièrement « *qu'aucune disposition de la loi ne permet de réduire, en raison d'une négligence de la victime, le montant des réparations civiles dues à celle-ci par l'auteur d'une infraction intentionnelle contre les biens, le délinquant ne pouvant être admis à bénéficier, fût-ce moralement de l'infraction* » (Cass. crim., 16 mai 1991, pourvoi n° 90-82285 ; *Bull. crim.* 1991, n° 208 ; *JCP* 1992, éd. G., I. 3572, obs. G. Viney. – Cass. crim., 28 févr. 1990, *RTD* civ. 1990, p. 670, obs. P. Jourdain. – Cass. crim., 4 oct. 1990 *; Bull. crim.* 1990, n° 331 ; *JCP* 1991, éd. G., IV. 8. – Cass. crim., 7 nov. 2001, pourvoi n° 01-80592 ; *Bull. crim.* 2001, n° 230 ; *RTD civ*. 2002, p. 314, obs. P. Jourdain ; *LPA* 16 oct. 2002, n° 207, p. 15 et s., note B. Jaluzot).

minimiser son dommage dans l'intérêt du responsable [1409], se démarquant ainsi des droits de la *Common law* qui reconnaissent, à la charge de la victime, un *duty to mitigate*.

2. Les limites de l'action en responsabilité délictuelle

467. Si la mise en œuvre des conditions de la responsabilité civile en matière de *spamming* ne semble pas poser de difficultés particulières, la question de son efficacité semble plus douteuse. Ce scepticisme résulte de plusieurs constats.

468. Une action inadéquate pour réparer les dommages mineurs subis par les « spammés ». Tout d'abord, au regard du très faible contentieux porté jusqu'à présent devant les tribunaux nationaux, les « spammés » français semblent peu enclins à engager une action en justice. Ce constat peut s'expliquer en raison des risques de s'exposer à une procédure longue et coûteuse par rapport au préjudice subi lequel se révèle minime, lorsqu'il touche des internautes, simples particuliers. En effet, hormis les hypothèses où le « spammeur » enverrait massivement des *spams* à une seule et unique personne dans le seul dessein de lui nuire [1410], le *spamming* constitue avant tout une pratique dommageable aux effets diffus. En effet, rappelons que le « spammeur » aura fréquemment recours à des logiciels de *push* permettant de toucher indistinctement un nombre très important de personnes. À l'occasion de cette opération d'envoi massif, chaque destinataire ne recevra en réalité qu'un seul *spam* provenant du même « spammeur » [1411]. Le préjudice personnel éprouvé par chaque

[1409] Cass. civ. 2e, 19 juin 2003 (2 arrêts), pourvois n° 01-13289 et 00-22302 ; *Bull. civ*. I n° 203 ; *D.* 2003, jurispr., p. 2326, note J.-P. Chazal ; *RTD* civ. 2003, p. 716, n° 3, note P. Jourdain. – Cass. civ. 2e, 8 oct. 2009, pourvoi n° 08-18492, *inédit.* – V. toutefois, Civ. 2e, 22 janv. 2009, pourvois n° 07-20878 08-10392 ; *Bull. civ*. II, n° 26 ; *D.* 2009, p. 1114, note R. Loir. – Pour une critique de cette solution, v. Muriel FABRE-MAGNAN, *Responsabilité civile et quasi-contrats*, *op. cit.*, spéc. pp. 375-376 (« *un juste milieu pourrait être trouvé entre l'obligation de modération de la Common law, excessivement exigeante vis-à-vis des victimes, et une solution qui laisse à ces dernières la possibilité d'alourdir avec insouciance la note du responsable* »). – Jacques FLOUR, Jean-Luc AUBERT, Éric SAVAUX, *Le fait juridique*, *op. cit.*, spéc. n° 387, p. 474 et s. (« La solution est sans doute contestable en ce qu'elle est sans nuances. On peut comprendre que la victime n'ait pas d'obligation de réduire le dommage qui lui a été infligé et qui est purement le fait de l'auteur. En revanche, il conviendrait sans doute de réserver les cas où la victime dispose de moyens sûrs et sans inconvénients pour elle ne pas laisser s'aggraver le dommage »). – V. ég. le projet CATALA qui propose de modérer l'étendue du dommage en cas de négligence de la victime : « *lorsque la victime avait la possibilité, par des moyens sûrs, raisonnables et proportionnés, de réduire l'étendue de son préjudice ou d'en éviter l'aggravation, il sera tenu de son abstention par une réduction de son indemnisation, sauf lorsque les mesures seraient de nature à porter atteinte à son intégrité physique* » (art. 1373). – Sur cette disposition, v. Jean-Luc AUBERT, « Quelques remarques sur l'obligation pour la victime de limiter les conséquences dommageables d'un fait générateur de responsabilité : À propos de l'article 1373 de l'avant-projet de réforme du droit des obligations », *in Études offertes à Geneviève VINEY*, *op. cit.*, spéc. p. 55 et s.

[1410] Tel sera le cas lorsqu'une victime subit une attaque de *mail bombing* ou lorsqu'un poste informatique, transformé en PC zombie, reçoit tous les messages expédiés depuis son poste et qui lui sont retournés.

[1411] V. *supra :* n° 44 et s.

« spammé » est donc tout à fait insignifiant [1412]. Il en résulte que même si les « spammés », simples particuliers, envisageaient d'engager une action en justice, le succès de leur action risque d'être fortement compromis dans la mesure où la Cour de cassation refuse généralement d'indemniser des préjudices d'un montant dérisoire [1413].

469. Les insuffisances de la réparation intégrale au regard de ses effets. S'agissant des effets de cette action sur les « spammeurs », ils risquent d'être très limités et ce, pour plusieurs raisons. Le coût dérisoire des envois de *spams*, l'inaction des victimes et le faible risque d'indemnisation auquel s'expose le « spammeur » font du *spamming* une pratique particulièrement lucrative. En effet, en mettant en balance le montant de l'indemnisation auquel il risque d'être condamné et le profit substantiel qu'il peut retirer de son activité, le résultat largement positif en sa faveur ne le dissuadera aucunement de renoncer à la poursuite de ses envois. Dans ce contexte, il semble donc incontestable que la responsabilité civile délictuelle, limitée à une fonction indemnitaire, se révèle largement insuffisante pour contrer ce type de comportement animé par l'appât du gain.

470. Bilan et perspectives d'amélioration. Pour assurer l'effectivité de l'action en responsabilité civile délictuelle, une réflexion doit donc s'engager autour de trois axes majeurs : la prise en compte du caractère lucratif du *spamming*, la nécessité de dépasser la fonction indemnitaire classique de la responsabilité civile et enfin, la prise en compte du caractère diffus du dommage causé. Pour répondre à ces différents objectifs, il est tout d'abord impératif de reconsidérer le droit de la responsabilité civile de façon telle qu'il permette de paralyser le bénéfice issu du *spamming*. Il est en effet avéré que le « spammeur » ne cessera ses envois que si cette pratique n'apparaît plus lucrative, c'est-à-dire si le coût des envois devient supérieur au gain engrangé [1414]. Par ailleurs, afin de mettre fin à une situation inacceptable dans laquelle les « spammeurs » profitent d'une activité lucrative au préjudice de milliers de personnes, il est essentiel que les victimes, en particulier celles exposées à un

[1412] En effet, le plus souvent, chaque « spammé » ne recevra qu'un seul message en provenance du même « spammeur ». Dans ces conditions, cet envoi non sollicité suscitera tout au plus une gêne, voire un agacement de la part de son destinataire.

[1413] V. par ex. Cass. civ. 1re, 24 juin 1986, pourvoi n° 84-15215, *Bull. civ.* I, n° 178 (énonçant qu'après avoir relevé que, d'après les documents produits, des impenses étaient d'un montant infime, une cour d'appel justifie par là même sa décision de ne pas en tenir compte). – Cass. civ. 1re, 4 avr. 1991, pourvoi n° 89-1711, *Bull. civ.* I, n° 127 (« *Mais attendu qu'ayant relevé le caractère insignifiant du fait invoqué, la cour d'appel a pu estimer qu'un tel fait n'avait pas causé à la SCI un préjudice ouvrant droit à indemnisation* »).

[1414] Pour une remarque similaire, v. Geneviève VINEY, « Rapport de synthèse » *in* « Faut-il moraliser le droit français de la réparation du dommage ? (À propos des dommages et intérêts punitifs et de l'obligation de minimiser son propre dommage) », colloque Paris 5, 21 mars 2002, *LPA* 20 nov. 2002, n° 232, p. 66 et s., spéc. p. 66 (« *Le besoin d'une sanction qui ne soit pas enfermée dans le cadre rigide du droit pénal et qui ne prenne pas seulement en compte le besoin d'indemnisation de la victime, mais aussi le profit tiré par l'auteur de son acte ainsi que la nocivité de son comportement, se fait sentir de plus en plus fortement aujourd'hui, notamment en droit de la concurrence, de la presse, de l'environnement et bien d'autres* »).

préjudice d'un montant infime, bénéficient d'une action adéquate leur permettant de poursuivre les « spammeurs ».

§ 3. LE *SPAMMING*, UNE OCCASION DE REPENSER UN DROIT DE LA RESPONSABILITÉ CIVILE PLUS ADAPTÉ

471. Comme nous venons de le voir, les insuffisances du droit de la responsabilité civile délictuelle invitent à envisager certains aménagements possibles qui lui permettraient de s'imposer comme un fondement d'action efficace pour les « spammés ». Nous verrons que les propositions d'évolutions vers lesquelles devraient tendre notre droit s'insèrent dans le sillage de discussions déjà amorcées, notamment dans le projet CATALA [1415], et qui semblent d'une acuité toute particulière en matière de *spamming*. Le débat, né autour de la reconnaissance en droit français de la faute lucrative, paraît retrouver toute sa vigueur en matière de *spamming* (A.). La consécration officielle de ce type de faute conduirait alors à déterminer comment celle-ci pourrait être sanctionnée pour s'affirmer comme un fondement d'action réellement efficace pour effacer des profits réalisés au préjudice des « spammés ». Cette question renvoie à examiner l'opportunité d'introduire en droit de la responsabilité civile français des dommages-intérêts punitifs, institution de droit étranger (B.). Nous verrons que les influences étrangères, pour repenser notre droit de la responsabilité civile adapté au problème du *spamming*, dépassent cette seule question et pourront être une source d'inspiration intéressante s'agissant de la forme d'action à mener. Plus précisément, dans l'hypothèse où le dommage subi est mineur, la consécration d'une action de groupe en droit français, à l'instar de celle existant en droit étranger, pourrait inciter les victimes d'un même dommage à se solidariser et empêcher d'être à nouveau victime des agissements de ce « spammeur » (B.).

A. L'OPPORTUNITE D'INTRODUIRE LA FAUTE LUCRATIVE

472. Après avoir défini ce que recouvre la notion de « faute lucrative » et ses possibles transpositions à l'hypothèse du *spamming* (1.), nous démontrerons la nécessité de sa reconnaissance officielle (2.).

[1415] Projet CATALA préc.

1. Définition et transposition à l'hypothèse du *spamming*

473. La définition jurisprudentielle. Absente du Code civil, la faute lucrative a été définie par la doctrine comme une faute « *qui, malgré les dommages et intérêts que le responsable est condamné à payer – et qui* [est] *calqu*[ée] *sur le préjudice subi par la victime – laiss*[e] *à leur auteur une marge bénéficiaire suffisante pour qu'il n'ait aucune raison de ne pas* [la] *commettre* » [1416]. C'est donc une « *faute qui rapporte* » [1417], qui consiste à « *ne viser personne en particulier, son auteur poursuivant tout simplement un but égoïste sans se soucier des conséquences pour les autres* » [1418]. Certaines des justifications qui sous-tendent l'existence de la faute lucrative sont très proches de celles qui motivent les agissements du « spammeur », notamment deux d'entre elles. En effet, la faute lucrative est une « *faut*[e] *intelligent*[e] » [1419] puisqu'elle « *est généralement la conséquence d'un calcul* » [1420]. Précisément en matière de *spamming*, en confrontant le gain espéré au montant de la réparation auquel il pourrait être condamné, le résultat obtenu, largement bénéfique pour ce dernier, ne pourra que l'inciter à poursuivre son activité. Par ailleurs, la persistance de cette faute lucrative peut parfois résulter du renoncement des victimes à saisir les tribunaux, ces derniers estimant que « *le préjudice, pris isolément, n'en vaut pas la peine* » et craignent ainsi de s'exposer à un procès long et coûteux [1421]. Cette circonstance pourra tout particulièrement se vérifier en matière de *spamming*, lorsque les internautes, simples particuliers, ne subissent qu'une gêne tout à fait mineure à la suite de la réception d'un, ou parfois, de quelques *e-mails* non sollicités, provenant d'un même « spammeur ».

[1416] Boris STARK, Henri ROLAND et Laurent BOYER, *Responsabilité délictuelle, op. cit.*, spéc. n° 1335, p. 534 (déplorant l'interdiction de prendre en compte la gravité de la faute tout particulièrement lorsque l'on se trouve en présence d'une faute lucrative). – Raymond LINDON, dénonçant les fautes lucratives pour demander leur prise en compte par le droit civil français, mettait l'accent sur le fait qu'« [i]*l est des directeurs de publications spécialisées dans la révélation des secrets d'alcôve qui, avant de publier une indiscrétion ou une photographie dont ils savent qu'elle leur vaudra un procès ou une condamnation, consultent leur avocat sur le montant probable de cette dernière et qui après avoir comparé cette évaluation à leur chiffre d'affaires, prennent allègrement la responsabilité d'encourir les foudres quelque peu mouillées de la justice* » (v. note sous CA Paris, 13 févr. 1971, *JCP* 1971, éd. G., II. 16774).

[1417] Juliette MEADEL, « Faut-il introduire la faute lucrative en droit français ? », *LPA* 17 avril 2007, n° 77, p. 6 et s., spéc. p. 6.

[1418] Daniel FASQUELLE, « L'existence de fautes lucratives en droit français », *in* colloque Paris 5 préc., *LPA* 20 nov. 2002, n° 232, p. 27 et s., spéc. n° 9, p. 29.

[1419] Suzanne CARVAL, « Vers l'introduction en droit français de dommages intérêts punitifs ? », *RDC*, p. 822 et s., spéc. p. 822.

[1420] v. Daniel FASQUELLE, « L'existence de fautes lucratives en droit français », art. préc., spéc. n° 15, p. 30. – V. ég. Philippe LE TOURNEAU, *Droit de la responsabilité et des contrats*, *op. cit.*, spéc. n° 48-1, p. 34 (la faute lucrative est « *celle qui laisse à son auteur une marge suffisante, une fois le paiement des dommages et intérêts, pour qu'il n'y ait aucune raison économique de ne pas la commettre* […]. *Elle résulte donc généralement d'une évaluation préalable de l'agent* »). – Juliette MEADEL, « Faut-il introduire la faute lucrative en droit français ? », art. préc., spéc. n° 10, p. 7 (« *La faute lucrative suppose un calcul : une évaluation entre le coût d'une procédure judiciaire et les gains obtenus par la violation de la loi ou de la morale* »).

[1421] Sur cet aspect de la faute lucrative, v. Daniel FASQUELLE, art. préc., spéc. n° 15, p. 30.

2. La nécessité d'une reconnaissance officielle

474. La multiplication des cas de fautes lucratives. La faute lucrative s'est développée principalement dans trois domaines. En matière d'atteintes à la vie privée (droit au respect de la vie privée, droit à l'image, à l'honneur ou à la considération, etc.), les fautes lucratives s'illustrent dans les nombreux litiges dans lesquels les organes de presse « à scandales » sont régulièrement poursuivis pour avoir diffusé des photos ou informations relatives à la vie privée de personnes célèbres afin de s'assurer des profits substantiels au préjudice de ces individus [1422]. Dans le domaine les actes de concurrence déloyale et de parasitisme économique [1423], le rapport de 2009 donne un exemple très éclairant d'un cas de faute lucrative dans le domaine de la concurrence et droit de la consommation et relatif à la surfacturation de quelques centimes d'euros les clients des opérateurs de téléphonie mobile. Ces clients qui représentent des centaines voire des millions de factures permettent ainsi de gagner des bénéfices très importants qui ne peuvent être neutralisés par les seuls dommages et intérêts compensatoires [1424]. Enfin, la violation des droits de propriété intellectuelle constitue une autre manifestation de la faute lucrative [1425]. La contrefaçon de marque ou de brevet, par exemple, permet à certains contrefacteurs de réaliser des gains parfois très importants s'ils ne sont condamnés qu'à hauteur du gain manqué par la victime et évalué selon les capacités de production de cette dernière alors que le contrefacteur disposent de moyens de production nettement plus performants. Outre ces domaines, la faute lucrative s'est largement étendue et est venue contaminer le droit des sociétés, le droit des assurances, le droit des transports, le droit de l'environnement et se retrouve encore dans le contentieux relatif à la rupture des contrats [1426]. Au regard de ces diverses manifestations de la faute lucrative, il devient dès lors urgent qu'elle soit prise en compte par le droit de la responsabilité civile car il est essentiel que leurs auteurs de telles fautes continuent à engranger des profits au préjudice des victimes.

475. La reconnaissance implicite de la faute lucrative par la jurisprudence et la loi. Cette évolution souhaitée vers la consécration officielle de la faute lucrative s'est déjà amorcée au sein de la jurisprudence et même de certaines dispositions légales. En effet, afin

[1422] Raymond LINDON, note sous CA Paris, 13 février 1971, note préc.
[1423] Marie-Anne FRISON-ROCHE, « Les principes originels du droit de la concurrence déloyale et du parasitisme », *RJDA* 6/94, p. 483et s. – Plus récemment, v. Daniel FASQUELLE et Rodolphe MESA, « La sanction de la concurrence déloyale et du parasitisme et le rapport Catala », *D.* 2005, chron., p. 2666 et s.
[1424] *Rapport d'information* n° 558 préc., spéc. p. 81.
[1425] Luc GRYNBAUM, « Une illustration de la faute lucrative : le " piratage " de logiciels », *D.* 2006, p. 655 et s. – Michel VIVANT, « Prendre la contrefaçon au sérieux », *D.* 2009, chron., p. 1839 et s.
[1426] Rodolphe MESA, « La consécration d'une responsabilité civile punitive : une solution au problème des fautes lucratives ? », *Gaz. Pal.* 21 nov. 2009, n° 325, p. 15 et s., spéc. p. 15.

de lutter contre ce type de faute, différentes manifestations jurisprudentielles démontrent la volonté des juges de prendre en compte ce type de faute et de neutraliser les avantages qu'elles procurent. Il en est ainsi lorsqu'à l'occasion de l'examen de la recevabilité de l'action en responsabilité, les juges ont consacré une appréciation souple des conditions de la responsabilité civile afin de faciliter la mise en œuvre de cette action [1427] ou lorsqu'ils fixent la réparation à un montant très élevé. En effet, en vertu du pouvoir souverain qui leur est conféré en la matière, les juges n'hésitent pas à prendre en compte divers éléments pour évaluer le préjudice tels que : la gravité de la faute, le profit réalisé [1428], voire même le gain espéré [1429] et ce, afin de punir l'auteur de la faute en le privant du bénéfice que cette dernière lui a procuré [1430]. De telles pratiques existent tout particulièrement lorsqu'il s'agit d'indemniser un préjudice moral. À cet égard, la doctrine majoritaire observe que « [l]*à où le dommage moral coexiste avec un dommage patrimonial, sa réparation a d'ailleurs souvent permis aux tribunaux, sans le dire, d'user de ce " chef de préjudice " pour augmenter les dommages et intérêts mis à la charge du responsable dans la mesure où, faisant remplir par l'indemnité une fonction de peine privée, ils ont estimé que l'attitude de l'auteur du dommage était nettement répréhensible* » [1431]. Cette volonté des juridictions judiciaires

[1427] Sur l'extension de la notion de dommage réparable, v. Christelle COUTANT-LAPALUS, *Le principe de la réparation intégrale en droit privé*, *op. cit.*, spéc. n° 496-500, p. 421-427. – V. ég. Daniel FASQUELLE, art. préc., spéc. n° 21, p. 30. – Philippe LE TOURNEAU, *Droit de la responsabilité et des contrats*, *op. cit.*, spéc. n° 48-1, p. 34.

[1428] En matière d'atteinte à la vie privée, certains auteurs sont favorables à la prise en compte des profits réalisés par les organes de presse et découlant de la vente d'articles dévoilant des éléments de la vie privée des personnes, v. not. Pierre KAYSER, *Remarques sur l'indemnisation du préjudice moral dans le droit contemporain*, *in Études offertes à Jean Macqueron*, P.U.A.M., 1970, p. 411 et s., spéc. n° 18 ; *La protection de la vie privée par le droit*, *op. cit.*, spéc. n° 201, pp. 370-371. – Raymond LINDON, note sous CA Paris, 13 févr. 1971, note préc.

[1429] Par ex. en matière de contrefaçon, en cas de faute lucrative, v. Suzanne CARVAL, *La responsabilité dans sa fonction de peine privée*, (préf. VINEY), tome 250, L.G.D.J., coll. *Bibl. dr. privé*, 1995, spéc. n° 130 et s., p. 135 et s. – Christelle COUTANT-LAPALUS, *Le principe de la réparation intégrale en droit privé*, *op. cit.*, spéc. nos 501-503, pp. 427-431. – V. ég. Philippe LE TOURNEAU, *Droit de la responsabilité et des contrats*, *op. cit.*, spéc. n° 47, p. 33 et les exemples cités en matière de contrefaçon, concurrence déloyale et parasitisme.

[1430] Sur les évolutions des modes de calcul du préjudice, v. Christelle COUTANT-LAPALUS, *Le principe de la réparation intégrale en droit privé*, *ibid.*, spéc. n° 501-505, pp. 427-434. – V. Daniel FASQUELLE, art. préc., spéc. n° 21, p. 30. – Geneviève VINEY souligne que « *tout le monde sait bien que se cache une pratique largement comparable à celle des dommages et intérêts punitifs ou exemplaires. Les juges cherchent à dissuader et, pour ce faire, ils calculent leur condamnation de manière à annuler les profits illicites* » (« Rapport de synthèse », *in* colloque Paris 5 préc., rapport préc., spéc. p. 67).

[1431] François TERRE, Philippe SIMLER et Yves LEQUETTE, *Les obligations*, *op. cit.*, spéc. n° 712, pp. 726-727. – V. ég. Suzanne CARVAL, *La responsabilité civile dans sa fonction de peine privée*, *op. cit.*, spéc. n° 21 et s., p. 23 et s. – Christelle COUTANT-LAPALUS, *Le principe de la réparation intégrale en droit privé*, *op. cit.*, spéc. n° 504, pp. 432-433. – Paul ESMEIN, « La commercialisation du dommage moral », *D.* 1954, chron., p. 113 et s. – Muriel FABRE-MAGNAN observe également que dans le cas d'un préjudice moral par ricochet, « [s'] *il peut parfois paraître inconvenant de mettre en avant la peine que l'on a de voir un être cher subir un dommage pour demander de l'argent en justice, l'admission de ce type de préjudice permet en réalité souvent de se servir de la responsabilité civile pour " punir " le responsable. On sait en effet que l'auteur d'un dommage ne peut être condamné qu'à réparer un préjudice qu'il a causé, si bien qu'accroître le nombre de préjudices indemnisables permet au juge (comme à la victime et à l'entourage) d'alourdir la condamnation en cas de comportement particulièrement répréhensible de l'auteur du dommage* » (*Responsabilité civile et quasi-contrats*, *op. cit.*, spéc. p. 126). – Jacques FLOUR, Jean-Luc AUBERT, Éric SAVAUX, *Le fait juridique*, *op. cit.*, spéc. n° 140, pp. 162-163 (« *La réparation du préjudice moral s'analyse en une peine privée. Il ne s'agit pas vraiment d'indemniser la victime – ou prétendue telle – mais de punir l'auteur* »). – Théodore IVAINER, « Le pouvoir souverain du juge

d'effacer les bénéfices a également pu se manifester à travers la publication des décisions de justice ou encore lorsque, dans le cadre d'un procès civil, des sommes particulièrement importantes sont prononcées au titre de l'article 700 du Code de procédure civile [1432]. La loi s'est elle-même attachée à sanctionner les profits illicites réalisés dans divers domaines : en matière de recel et de blanchiment où le montant des amendes est fixé en fonction du produit de l'infraction [1433], en cas de pratiques restrictives de concurrence, le Code commerce prévoit des sanctions complémentaires de la réparation telles que l'amende civile [1434] ou encore en matière d'indemnisation de la contrefaçon. À cet égard, plusieurs dispositions créées par la loi n° 2007-1544 du 29 octobre 2007 de lutte contre la contrefaçon [1435] sont relatives à l'évaluation des dommages et intérêts et permettent au demandeur d'intégrer, dans l'indemnité que le contrefacteur aura à lui verser, la restitution des bénéfices réalisés par ce dernier [1436].

476. Au regard de la multiplication des fautes lucratives et du développement d'une jurisprudence favorable à la reconnaissance de ce type de faute, il apparaît essentiel de l'intégrer officiellement dans notre droit français [1437]. Cette évolution permettrait non

dans l'appréciation des indemnités réparatrices », chron. préc. –Raymond LINDON, note sous CA Paris, 13 févr. 1971, *JCP* 1971, éd. G., II. 16774. – Henri, Léon et Jean MAZEAUD et François CHABAS, *Leçons de droit civil, Les obligations : théorie générale, op. cit.*, spéc. n° 623, p. 735 (observant que « *les juges se laissent souvent impressionner par la gravité de la faute lorsqu'ils fixent le chiffre des dommages-intérêts, plus particulièrement pour la réparation du préjudice moral, le plus difficile à évaluer* »). – Georges RIPERT, « Le prix de la douleur », *D.* 1948, chron., p. 1 et s. (« *sans doute la victime ne crie pas devant le juge son désir de vengeance pour ne pas avilir sa cause ; le juge ne dit pas dans sa sentence qu'il punit le coupable, parce qu'il a seulement le droit d'indemniser la victime ; mais le dessein de frapper l'auteur d'une faute est visible dans l'action du demandeur et la peine privée se cache sous la forme d'une indemnité quand le juge tient compte, pour en fixer le montant, de la gravité de la faute et de la fortune du défendeur* » (*id.*, spéc. p. 1). – Roger TRIBES, *Fondement et caractères de la réparation du préjudice moral*, Imprimerie du Palais, Nice, 1932 (favorable à l'idée de peine privée, cet auteur considère que le montant de la réparation du dommage moral doit être fixé en fonction de l'importance de la faute qui a causé le dommage (*id.*, spéc. p. 105). – Geneviève VINEY et Patrice JOURDAIN, *Les conditions de la responsabilité, op. cit.*, spéc. n° 254, p. 36 et s. – *Contra* Jean GANOT, *La réparation du préjudice moral*, Imprimerie Edoneur, Rennes, 1924 (souhaitant l'abandon définitif de l'idée de peine privée (*id.*, spéc. p. 224)).

[1432] Art. 700 C. proc. civ. : « […] *dans toutes les instances, le juge condamne la partie tenue aux dépens ou, à défaut, la partie perdante, à payer à l'autre partie la somme qu'il détermine, au titre des frais exposés et non compris dans les dépens. Le juge tient compte de l'équité ou de la situation économique de la partie condamnée. Il peut, même d'office, pour des raisons tirées des mêmes considérations, dire qu'il n'y a pas lieu à cette condamnation* ».

[1433] Art. 321-3 et 324-3 C. pén.

[1434] Art. L. 442-6 C. comm.

[1435] Tristan AZZI, « La loi du 29 octobre 2007 de lutte contre la contrefaçon : présentation générale », *D.* 2008, Dossier 700, p. 700 et s., spéc. n° 35 et s., p. 708 et s. – Pierre-Yves GAUTIER, « Fonction normative de la responsabilité : Le contrefacteur peut être condamné à verser au créancier une indemnité contractuelle par équivalent », *D.* 2008, Dossier, p. 727 et s. – Michel VIVANT, « Prendre la contrefaçon au sérieux », chron. préc. – Jacques HUILLIER, « Propriété intellectuelle : des dommages et intérêts punitifs pas si punitifs », *Gaz. Pal.* 5-7 juill. 2009, n° 188, p. 2270 et s.

[1436] Art. L. 331-1-3, al. 1er CPI en matière de propriété littéraire et artistique, art. L. 521-7, al. 1er CPI concernant les dessins et modèles, art. L. 615-7, al. 1er CPI relatif aux brevets, art. L. 716-14, al. 1er CPI pour les marques, art. 622-28-1, al. 1er CPI en matière d'obtention végétale et art. 722-6, al. 1er CPI pour les appellations d'origine et indications géographiques.

[1437] Du même avis, v. Daniel FASQUELLE, « L'existence de fautes lucratives en droit français », art. préc., spéc. n° 35, p. 34. – Également favorable à la consécration de la faute lucrative, Philippe LE TOURNEAU, *Droit de la*

seulement de ne pas laisser impunies des fautes d'une particulière gravité mais également de mettre fin à une jurisprudence fluctuante, source d'insécurité juridique. Enfin, cette solution attesterait que le Droit s'attache à prendre en compte des considérations d'ordre économique, ce qui reste encore trop rare en France comme le fait très justement remarquer le professeur Philippe LE TOURNEAU et répondrait ainsi à un souci d'efficacité du droit [1438].

477. Vers une reconnaissance officielle ? L'accroissement de la faute lucrative a d'ailleurs donné lieu à une véritable prise de conscience politique et institutionnelle de la nécessité de prendre en compte ce type de faute. Pour lever l'incertitude et la précarité actuelles qui entourent la faute lucrative, l'avant-projet de réforme du droit des obligations contient les germes de cette nouvelle perspective en consacrant la notion de « faute lucrative » [1439]. À cet égard, le professeur Geneviève VINEY, rédactrice de la partie du projet CATALA consacré à la responsabilité civile, a proposé d'introduire cette notion dans le Code civil [1440]. L'exposé des motifs de ce projet vient préciser ce qu'il convient d'entendre par cette notion. Il s'agit d'« *une faute dont les conséquences profitables pour son auteur ne seraient pas neutralisées par une simple réparation des dommages causés* » [1441]. De même, le rapport d'information de 2009 qui met en exergue le besoin de faire évoluer les règles en matière de responsabilité civile et plus récemment, plus récemment, la proposition de loi portant réforme de la responsabilité civile de 2010 s'inspirant directement des travaux de 2005 et de 2009, visent ce type de faute lorsqu'ils envisagent les effets de la responsabilité civile [1442].

---

responsabilité et des contrats, *op. cit.*, spéc. n° 48-1, p 34. – *Contra* Rodolphe MESA, « La consécration d'une responsabilité punitive : une solution au problème des fautes lucratives ? » art. préc. (estimant cette solution comme inopportune, et considérant que la seule façon d'appréhender les bénéfices réalisés par l'auteur du dommage passe par la consécration d'un principe de restitution intégrale des profits illicites, complémentaire du principe de réparation intégrale du préjudice).

[1438] Philippe LE TOURNEAU, *Droit de la responsabilité et des contrats*, *op. cit.*, spéc. n° 48-2, p. 35 (« *le mouvement Law and Economics (notamment de l'École de Chicago) a montré tout l'intérêt d'une telle démarche* [fondée sur une analyse économique du droit], *permettant de mesurer l'efficacité du Droit pour inciter à ne pas commettre de dommages. Un de ses axiomes (du reste de bon sens) est que le Droit doit être efficace : l'est-il lorsque des personnes (physiques ou morales) peuvent impunément le bafouer, y compris des décisions judiciaires ?* »). – V. Grégory MAITRE, *La responsabilité à l'épreuve de l'analyse économique du droit*, L.G.D.J., 2005.

[1439] Projet CATALA, préc., spéc. p. 148.

[1440] « *l'auteur d'une faute manifestement délibérée, et notamment d'une faute lucrative, peut être condamné, outre les dommages-intérêts compensatoires, à des dommages-intérêts punitifs* » (proposition d'article 1371 du C. civ.).

[1441] Geneviève VINEY, « De la responsabilité civile (articles 1340 à 1386) : exposé des motifs » *in* projet CATALA préc., spéc. p. 148. – V. dans le même sens, Alain ANZIANI et Laurent BETEILLE (présenté par), *Responsabilité civile : des évolutions nécessaires*, Rapport d'information, Doc Sénat n° 558, 15 juill. 2009, spéc. p. 80, disponible sur : http://www.senat.fr/rap/r08-558/r08-5581.pdf

[1442] Rapport d'information n° 558 préc., p. 80 et s. et son document de synthèse, disponible sur : http://www.senat.fr/rap/r08-558/r08-558-syn.pdf (« *Le droit français est fondé sur le principe de la réparation intégrale du dommage* […] [c]*ette approche paraît cependant inadaptée dans certains domaines face à des fautes dites " lucratives "* » (document de synthèse, spéc. p. 3)). – Proposition de loi portant réforme de la

3. La sanction de la faute lucrative : l'opportunité d'introduire des dommages-intérêts punitifs

478. Les effets découlant de la consécration juridique de la faute lucrative. Au regard de la pertinence de l'introduction de la faute lucrative dans le droit civil, se pose alors la question de sa sanction. Le régime de la responsabilité délictuelle tel qu'il existe actuellement, fondé sur la seule réparation du dommage subi, apparaît largement insuffisant pour appréhender ce type de faute. Nous rejoignons ainsi l'opinion du professeur Geneviève VINEY qui estime « *qu'il est non seulement souhaitable mais même, semble-t-il, nécessaire de permettre aux juges de dépasser une vision purement indemnitaire* » [1443]. En effet, comme nous l'avons souligné en matière de *spamming*, l'effacement du profit réalisé apparaît comme le seul gage d'une cessation de telles activités lucratives. La solution pourrait dès lors consister à prendre en compte non seulement le besoin d'indemnisation de la victime mais aussi la nocivité du comportement poursuivi, tout en s'assurant de ne pas enfermer la sanction dans un cadre trop rigide [1444]. Pour atteindre cet objectif, l'octroi de dommages-intérêts punitifs [1445], institution juridique empruntée aux pays de la *Common law* [1446], qui viendrait s'ajouter aux dommages et intérêts compensatoires destinés à réparer le dommage subi [1447] pourrait se révéler pertinente [1448]. Toutefois, la controverse quant à la consécration

responsabilité civile, proposition préc., proposition d'article 1386-25 du C. civ. : « *lorsque le dommage résulte d'une faute délictuelle* [qui] *a permis à son auteur un enrichissement que la seule réparation du dommage n'est pas à même de supprimer, le juge peut condamner* […] *l'auteur du dommage* […] *à des dommages et intérêts punitifs* ».

[1443] GenevièveVINEY, « L'appréciation du préjudice », *LPA* 19 mai 2005, n° 99, p. 89 et s., spéc. p. 90. – Selon Marie-Anne FRISON-ROCHE, (« *si la sanction susceptible d'être prononcée* […] *est en toute hypothèse d'un montant moindre que le profit immédiatement acquis, non seulement l'entreprise peut mais elle doit, par rationalité économique, enfreindre la loi* » (« Les principes originels du droit de la concurrence déloyale et du parasitisme », art. préc., spéc. n° 18, p. 495)). L'auteur préconise ainsi de prendre en compte « *la rationalité économique* » : « *Si l'on ne veut pas qu'il en soit ainsi, et que le droit se contente de facturer, avec retard, à l'entreprise le prix de son comportement économiquement profitable, il faut alors aller vers des sanctions au montant plus élevé que le quantum du dommage, ou aller vers des sanctions détachées du dommage, comme par exemple le discrédit porté socialement sur l'entreprise, par des mises au pilori modernes, telles que* [la] *publication dans les journaux, etc.* » (*id.*, n° 19, p. 495).

[1444] On rejoint ainsi la proposition du professeur Genviève VINEY qui consiste à « *mettre sur pied un cadre juridique à la fois suffisamment souple pour affranchir la sanction des contraintes excessives du droit pénal – principe de légalité, interprétation étroite des textes, … – et suffisamment strict pour éviter l'arbitraire des condamnations et leur cumul abusif avec d'autres sanctions civiles, pénales ou administratives* » (« Rapport de synthèse », *in* colloque Paris 5 préc., rapport préc., spéc. p. 67).

[1445] Sur cette notion, v. Stéphane PIEDELIEVRE, « Les dommages-intérêts punitifs : une solution d'avenir ? », *in* « La responsabilité civile à l'aube du XXI[e] siècle : Bilan prospectif – colloque Chambéry 7 et 8 déc. 2000 », *Resp. civ. assur*. juin 2001, n° 6 bis, étude 13, p. 68 et s.

[1446] Sur ce point, v. Camille JAUFFRET-SPINOSI, « Les dommages-intérêts punitifs dans les systèmes de droit étrangers », *in* colloque Paris 5 préc., *LPA* 20 nov. 2002, n° 232, p. 8 et s. – Plus particulièrement aux États-Unis, v. Jacques BOURTHOUMIEUX, « Dommages punitifs », *RGDA* 1996, p. 861 et s. – Suzanne CARVAL, *La responsabilité dans sa fonction de peine privée, op. cit.*, spéc. n° 15, p. 15 et n° 89 et s., p. 95 et s. (application en matière de produits défectueux).

[1447] Sur la distinction entre « dommages et intérêts » et « dommages-intérêts », v. Omid SAEDI, « Dommages-intérêts ou dommages et intérêts, celle-ci ou celle-là ; ou bien les deux », *LPA* 7 juin 2005, n° 12, p. 6 et s. (En pratique, les deux termes sont très souvent considérés comme synonymes. Toutefois, selon cet auteur, lorsque

de ce type de dommages-intérêts est si vigoureuse que l'exposé de ces critiques s'impose avant de démontrer que chacune d'entre elles n'est pas insurmontable (a.). Il s'agira ensuite de s'attacher à un examen plus technique destiné à envisager le régime qu'il conviendrait d'adopter en vue d'une réforme future du droit de la responsabilité civile délictuelle (b.).

a. Une réception controversée

479. Le dépassement de la fonction indemnitaire. L'introduction de ce type de dommages-intérêts implique inévitablement une évolution profonde de la fonction de la responsabilité civile puisqu'elle vise à acquérir une dimension punitive et non plus exclusivement indemnitaire. Cette conséquence inéluctable conduit certains à dénoncer cette proposition jugée comme incompatible avec la fonction réparatrice de la responsabilité civile [1449]. « *Cette orientation punitive est* [ainsi] *de nature à transformer la responsabilité civile en responsabilité parapénale, voire en " responsabilité pénale bis "* » [1450]. Ce « *mélange des genres entre le civil et le pénal* » [1451] serait de nature à créer une confusion entre les responsabilités civile et pénale alors même que l'une et l'autre poursuivent des objectifs clairement distincts : la première visant à réparer le dommage subi par la victime, la seconde à sanctionner le coupable. Si cette critique doit être prise en compte, elle ne saurait faire obstacle au principe même des dommages-intérêts non compensatoires [1452]. Plusieurs arguments viennent au soutien de cette affirmation. Tout d'abord, rappelons qu'en droit

l'objectif est indemnitaire, la réparation est assurée par des dommages et intérêts constitués de deux éléments distincts : la perte et le gain manqué. En revanche, lorsqu'il s'agit de sanctionner le fautif, ce dernier sera condamné aux versements de dommages-intérêts). Par souci de clarté de nos propos, nous adopterons cette même distinction.

[1448] On aurait pu également penser à recourir à l'amende civile mais à l'instar des sanctions pénales, celle-ci est plafonnée et limite fortement son efficacité en cas de fautes lucratives. Par ailleurs, Martine BEHAR-TOUCHAIS souligne « *les effets pervers de l'amende civile* » car son recours risque de priver la personne poursuivie des garanties offertes par le droit pénal en raison de l'imprécision des textes d'incrimination, du défaut d'interprétation stricte de ces textes et de l'absence de présomption d'innocence. Elle présente également des risques pour la victime qui ne peut la demander. L'auteur conclut en mettant en garde contre le recours à l'amende civile car le problème *« c'est qu'on veut quelque chose de paradoxal, à savoir " le droit pénal sans le droit pénal "* (« L'amende civile est-elle un substitut satisfaisant à l'absence de dommages et intérêts punitifs ? », *LPA* 20 nov. 2002, n° 232, p. 36 et s.).

[1449] V. not. Philippe BRUN, « Rapport introductif », *in* colloque Chambéry préc., *Resp. civ. assur.* juin 2001, n° 6 bis, p. 1 et s.

p. 1 et s. – Christian LAPOYADE-DESCHAMPS, « Quelle(s) responsabilité(s) ? », *in* colloque Chambéry préc., p. 62 et s. – Stéphane PIEDELIEVRE, « Les dommages-intérêts punitifs : une solution d'avenir ? », *in* colloque Chambéry préc., étude préc., spéc. n° 22, p. 72 (considérant l'admission des dommages-intérêts punitifs dans le droit de la responsabilité civile comme « *une fausse bonne idée* »). – Robert SAINT-ESTEBEN, « Pour ou contre les dommages et intérêts punitifs », *LPA* 20 janv. 2005, n° 14, p. 53 et s.

[1450] Rodolphe MESA, « La consécration d'une responsabilité civile punitive : une solution au problème des fautes lucratives ? », art. préc., spéc. p. 17.

[1451] Rodolphe MESA, art. préc., spéc. p. 16. – Robert SAINT-ESTEBEN, « Pour ou contre les dommages et intérêts punitifs », art. préc.

[1452] Geneviève VINEY, « Quelques propositions de réforme du droit de la responsabilité civile », *D.* 2009, p. 2944 et s., spéc. p. 2946.

positif, il existe quatre mesures officiellement qualifiées de peine privée, à savoir : la clause pénale, l'astreinte, les règles régissant la solidarité entre les co-responsables et les mesures de déchéance [1453], ce qui témoigne incontestablement de « *la survivance de cette notion au sein du droit privé français* » [1454]. En outre, plusieurs travaux doctrinaux ont mis en évidence que la fonction de peine privée de la responsabilité civile conserve toujours une certaine vigueur au cours des époques [1455]. Le professeur Boris STARK a souligné à cet égard que le système des peines privées opérait selon un mode cyclique : « *le mouvement d'abolition de la peine privée s'accompagne d'un mouvement inverse qui tend à la rétablir. Tel le phénix, la peine privée ne meurt que pour renaître* » [1456]. Cette réapparition ponctuelle de la peine privée se manifeste dans certaines hypothèses où la recherche de solutions efficaces commande le dépassement de la fonction traditionnelle de la responsabilité civile pour contrarier les calculs opérés par l'auteur de la transgression. Cet impératif transparaît clairement à travers les arrêts qui s'évertuent à neutraliser les bénéfices escomptés par le fautif. De même, le mode de calcul des dommages et intérêts en matière de contrefaçon illustre l'abandon du principe d'équivalence entre le dommage subi et le montant de la réparation allouée. La prise en compte de la faute lucrative par la jurisprudence ainsi que par la loi et les effets qui s'y attachent – notamment, une réparation supérieure au dommage subi – démontre sans conteste que la responsabilité civile endosse d'ores et déjà dans certaines hypothèses un rôle répressif [1457]. Dans ces circonstances, il est permis de supposer, et d'espérer, que l'impératif d'efficacité qui a justifié une évolution en matière de contrefaçon [1458], « *pourrait être appelée à retentir … sur le droit commun de la responsabilité* » [1459].

480. L'atteinte au principe de la réparation intégrale. Les opposants à une éventuelle évolution de la fonction de la responsabilité civile soutiennent que la reconnaissance d'une fonction pénale porterait atteinte au principe de la réparation intégrale. Cette critique résulte non seulement du montant des dommages-intérêts punitifs qui dépassera nécessairement celui du préjudice subi mais également de la prise en compte de la

[1453] Christelle COUTANT-LAPALUS, *Le principe de la réparation intégrale en droit privé, op. cit.,* spéc. n[os] 480-494, pp. 407-420.
[1454] Christelle COUTANT-LAPALUS, *ibid*., spéc. n[o] 494, p. 420.
[1455] V. par. ex. Louis HUGUENEY, « Le sort de la peine privée en France dans la première moitié du XX[e] siècle », *in Le sort de la peine privée au milieu du XX[e] siècle, Études offertes au professeur RIPERT,* tome 2, L.G.D.J., coll. *Mélanges*, 1950, p. 249 et s. – Plus récemment, Suzanne CARVAL, *La responsabilité civile dans sa fonction de peine privée*, *op. cit.* – V. ég. Alexis JAULT, *La notion de peine privée, op. cit.*
[1456] Boris STARCK, *Essai d'une théorie générale de la responsabilité considérée en sa double fonction de garantie et de peine*, thèse Paris, sous la direction de Maurice PICARD, éd. Rostein, 1947, spéc. p. 377.
[1457] À cet égard, Christelle COUTANT-LAPALUS évoque une « *application latente de la peine privée* » (*Le principe de la réparation intégrale en droit privé*, *op. cit*., spéc. n° 495 et s., p. 420 et s.).
[1458] Michel VIVANT, « Prendre la contrefaçon au sérieux », chron. préc.
[1459] Pierre-Yves GAUTIER, « Fonction normative de la responsabilité », dossier préc.

faute plutôt que celle du dommage, conduisant ainsi « *à un amenuisement du rôle du préjudice* » [1460] . Le principe de la réparation intégrale, qui commande de réparer tout le dommage et rien que le dommage, serait *a priori* bel et bien bafoué. Toutefois en pratique, une analyse attentive de la jurisprudence démontre que le dogme de la réparation intégrale n'est pas inébranlable et doit être relativisé, les juges ayant tendance à s'écarter de ce principe [1461]. Comme le souligne le professeur Geneviève VINEY, « *le prétendu principe de réparation intégrale* […] *est bien souvent un leurre.* [S]*on application est, dans certains domaines, tout simplement impossible. C'est le cas à chaque fois qu'il s'agit d'un dommage moral par définition inévaluable en argent* » [1462]. De surcroît, le principe de la réparation intégrale n'est pas d'ordre public [1463] et conduit certains auteurs à fortement relativiser la force de ce principe [1464]. Il apparaît dès lors que les nombreuses limites auxquelles se heurte le principe de la réparation intégrale permettent de soutenir que l'introduction de dommages-intérêts en droit français ne sera pas de nature à « *bouleverser la portée de ce principe* » [1465].

481. L'enrichissement sans cause de la victime. La consécration officielle des dommages-intérêts punitifs ferait courir, selon certains, le risque d'un enrichissement sans cause de la victime. À cet égard, le professeur Daniel FASQUELLE attire l'attention sur le fait que « [s]*'il est indispensable de prendre en compte les fautes lucratives en droit positif français, on veut mettre en garde, cependant, contre certains effets pervers possibles des solutions retenues. En particulier, il faut éviter un enrichissement des victimes qui, outre qu'il serait sans fondement et provoquerait une multiplication des actions en justice, pourrait venir perturber le bon fonctionnement de la justice* » [1466]. Toutefois, comme l'explique de façon astucieuse le professeur Suzanne CARVAL, il est permis d'y voir non pas forcément un « *enrichissement immérité* » mais plutôt « *une rémunération* » qui a vocation à

[1460] Stéphane PIEDELIEVRE, « Les dommages-intérêts punitifs : une solution d'avenir ? », *in* colloque Chambéry préc., étude préc., spéc. n[os] 13-15, pp. 70-71.
[1461] Sur l'admission des dommages-intérêts punitifs par la jurisprudence, v. not. Patrice JOURDAIN, « Rapport introductif » *in* colloque Paris 5 préc., *LPA* 20 nov. 2002, n° 232, p. 3 et s., spéc. p. 4.
[1462] Geneviève VINEY, « Rapport de synthèse » *in* colloque Paris 5 préc., rapport préc., spéc. p. 67.
[1463] Christelle COUTANT-LAPALUS, *Le principe de réparation intégrale en droit privé, op. cit.*, n° 122 et s., p. 121 et s.
[1464] Le professeur Boris STARCK observe que « *dans l'immense majorité des cas, la théorie de la réparation intégrale est tout simplement inconcevable sur le terrain délictuel.* […] *l'indemnité accordée pour le prix de la douleur n'est qu'une satisfaction approximative. Parler en ces matières de réparation intégrale, c'est proposer une formule vide de toute substance* » (*Essai d'une théorie générale de la responsabilité civile considérée en sa double fonction de garantie et de peine privée*, thèse préc., spéc. p. 404).
[1465] V. en ce sens, Juliette MEADEL, « Faut-il introduire la faute lucrative en droit français ? », art. préc., spéc. n° 22, p. 6 (« *Le principe de réparation intégrale connaît donc des limites ; l'introduction de la faute lucrative ne devrait pas bouleverser la portée de ce principe déjà fortement mis à mal par la somme des exceptions qu'il connaît* »).
[1466] Daniel FASQUELLE, « L'existence de fautes lucratives en droit français », art. préc., spéc. n[o] 35, p. 34.

récompenser l'initiative du demandeur ayant permis au juge de connaître de l'existence de cette faute et de sanctionner son auteur [1467].

482. L'opportunité de consacrer officiellement les dommages-intérêts punitifs. Sans mésestimer la réalité de ces arguments, la consécration en droit civil des dommages-intérêts punitifs, un des « *modes traditionnels d'expression de la peine privée* » [1468], se révèle, selon nous, opportune. En effet, il apparaît inacceptable de constater qu'une forte proportion de responsables tire profit d'un comportement fautif commis au préjudice de leurs victimes en toute impunité faute de sanction efficace et dissuasive. Malgré les oppositions à leur introduction, cette solution se présenterait comme une réponse adéquate au regard des effets produits sur les responsables. D'une part, ils pourraient avoir un effet dissuasif, en particulier lorsqu'ils sont évalués sur la base des profits réalisés puisque leur effacement anéantirait tout l'intérêt qui justifiait l'exercice de leur activité et auraient de fortes chances de décourager les condamnés à recommencer. D'autre part, ils peuvent avoir un effet préventif lorsque la condamnation à des dommages-intérêts punitifs fait l'objet d'une large publicité puisqu'une telle mesure pourrait dissuader de façon efficace ceux qui envisageraient d'entreprendre des activités similaires [1469]. Par ailleurs, à l'instar de toute peine privée, les dommages-intérêts punitifs permettent de pallier une sanction pénale insuffisante ou inefficace [1470]. Enfin, à l'égard des victimes, ils viendraient compenser les effets d'une indemnisation le plus souvent symbolique en raison des difficultés d'évaluation du dommage [1471]. Au regard des mérites que l'on peut prêter aux dommages-intérêts punitifs, leur reconnaissance implicite par les juges ne doit pas continuer à se poursuivre à demi-mot, l'imprévisibilité des solutions crée une situation d'insécurité juridique pour les victimes que plusieurs auteurs dénoncent à juste titre [1472]. Pourquoi ne pas assumer le fait que le droit de la

[1467] Suzanne CARVAL, *La responsabilité civile dans sa fonction de peine privée*, *op. cit.*, spéc. n° 318, p. 362.
[1468] Christelle COUTANT-LAPALUS, *Le principe de la réparation intégrale en droit privé*, *op. cit.*, spéc. n° 466, p. 395.
[1469] Patrice JOURDAIN, « Rapport introductif », rapport préc., spéc. n° 9, p. 4.
[1470] V. sur ce point, Geneviève VINEY, « Quelques propositions de réforme du droit de la responsabilité civile », art. préc., spéc. p. 2945.
[1471] Patrice JOURDAIN, « Rapport introductif », rapport préc., spéc. n° 9, pp. 4-5.
[1472] Daniel FASQUELLE, « L'existence de fautes lucratives en droit français », art. préc., spéc. n^{os} 24-25, p. 32. – Geneviève VINEY, « Rapport de synthèse », *in* colloque Chambéry préc., p. 82 et s., spéc. n^{o} 28, p. 86 (« *le pouvoir souverain des juges du fond* […] *– qui devrait, de toute évidence, exiger une motivation très précise des décisions des cours d'appel sur ce point – conduit* […] *à une insécurité généralisée qui favorise une litigation excessive* »). Elle ajoute qu'« *il s'agit là d'une pratique occulte et par conséquent non contrôlée, ce qui la fragilise et favorise toutes les dérives* » (*idem*, spéc. p. 67). – Philippe LE TOURNEAU, *Droit de la responsabilité et des contrats*, *op. cit.*, spéc. n° 45, p. 31 (« *en pratique, les tribunaux n'hésitent pas à condamner à des dommages et intérêts considérables certains auteurs de dommages, parce qu'ils savent que, finalement, le poids en sera supporté par l'assureur, donc dilué. Cette pratique n'est pas saine. Si nous souhaitons l'instauration d'un pouvoir " aggravateur ", c'est d'une autre manière qu'il faut l'entendre. Les dommages et intérêts majorés ne doivent pas être alloués en contemplation de l'intérêt que présente la victime, et en pensant que l'assureur paiera, mais afin de punir d'une façon particulière l'auteur du dommage, lorsque sa faute paraît extrêmement grave.* […] *Et de souhaiter une large reconnaissance de la possibilité pour le juge d'infliger dans cet esprit une peine privée* »).

responsabilité peut évoluer et doit évoluer au gré des besoins ?, cette voie semble indispensable si l'action en responsabilité délictuelle veut se maintenir comme une action effective. Ainsi, plutôt que de s'évertuer à résister à une évolution déjà largement amorcée et de masquer une fonction de peine privée déjà assumée par la responsabilité civile, il serait plus judicieux de réfléchir à l'élaboration d'un régime applicable à cette institution permettant de dégager des solutions prévisibles, gage de sécurité juridique et de lever les incertitudes quant à sa mise en œuvre.

b. La question du régime des dommages-intérêts punitifs

483. Si l'introduction de dommages-intérêts punitifs est considérée comme pertinente, il convient de s'interroger sur l'efficacité de cette institution telle que proposée par le projet CATALA : « *L'auteur d'une faute manifestement délibérée, et notamment d'une faute lucrative, peut être condamné, outre les dommages-intérêts compensatoires, à des dommages-intérêts punitifs* » [1473]. Cette proposition a été reprise dans les conclusions du rapport d'information de 2009 qui, favorable à l'introduction de dommages-intérêts punitifs, préconise d'« *autoriser les dommages et intérêts punitifs en cas de faute lucrative dans certains contentieux spécialisés* » [1474]. La proposition de loi de 2010 ouvre également « *la voie au prononcé par le juge, en plus de dommages et intérêts visant à compenser le préjudice, de dommages et intérêts punitifs dans les seuls cas où la loi l'autorise expressément et à l'égard des seules fautes lucratives* » [1475].

484. Domaine limité à la faute lucrative. Selon ces différents travaux, l'octroi de dommages-intérêts punitifs est subordonné à la caractérisation d'une faute spécifique, une « *faute manifestement délibérée* ». Étrangère aux catégories de faute connues du droit de la responsabilité, elle tend à se rapprocher de la faute intentionnelle sans toutefois se confondre avec cette dernière qui implique « *la volonté de l'acte déviant lui-même, mais encore une volonté orientée vers le résultat dommageable* » [1476]. Or, comme nous l'avons vu à

[1473] V. projet CATALA préc., art. 1371.
[1474] Rapport d'information n° 558 préc., spéc. recommandation n° 24 préc.
[1475] Proposition de loi portant réforme du droit de la responsabilité civile, proposition préc., spéc. p. 6 ; v. proposition d'article 1386-25 du C. civ. : « *lorsque le dommage résulte d'une faute délictuelle ou d'une inexécution contractuelle commise volontairement et a permis à son auteur un enrichissement que la seule réparation du dommage n'est pas à même de supprimer, le juge peut condamner, par décision motivée, l'auteur du dommage, outre à des dommages et intérêts en application de l'article 1386-22, à des dommages et intérêts punitifs* ».
[1476] Muriel CHAGNY, « Une (r)évolution du droit français de la concurrence ? – À propos de la loi LME du 4 août 2008 », chron. préc.

l'occasion de l'examen préalable de la faute lucrative, celle-ci est orientée vers la réalisation de bénéfices et non vers l'intention de commettre un dommage.

485. La question de l'affectation des dommages-intérêts punitifs. Le projet CATALA propose d'octroyer une part des dommages-intérêts punitifs à la victime et d'accorder au « *juge* […] *la faculté de faire bénéficier pour une part le Trésor public* » [1477]. L'affectation à la victime a le mérite de répondre de façon cohérente à la notion de peine privée qui doit être, par définition, versée à la victime. S'agissant de l'attribution d'une fraction du montant de ces dommages-intérêts au Trésor public, cette solution permettrait d'apaiser les craintes quant à un enrichissement sans cause de la victime [1478]. Toutefois, si le principe d'une affectation divisée apparaît souhaitable, l'attribution au Trésor public reste critiquable en ce sens qu'il tend à semer le trouble ente les catégories, l'amende civile étant elle-même affectée au Trésor public [1479]. De plus, elle risque d'entraîner une remise en cause de l'appartenance des dommages-intérêts punitifs à la catégorie de peine privée en créant une confusion avec le droit pénal. Or, le contentieux relatif à la peine privée doit rester exclusivement privé et ne peut, par conséquent être attribué au Trésor public. Pour surmonter ces difficultés, la solution pourrait alors consister à affecter cette fraction non attribuée à la victime à un fonds d'indemnisation tel qu'il est proposé dans le rapport d'information de 2009 [1480] ou par la proposition de loi de 2010 [1481]. Un Fonds général de garantie serait opportun puisqu'il permettrait de ne pas multiplier le nombre de fonds spéciaux déjà important [1482].

486. La question de l'assurance. Il s'agit ici de déterminer si le responsable peut s'assurer contre une sanction punitive qui serait prononcée à son encontre. La réponse est

[1477] V. projet CATALA préc., art. 1371.
[1478] Également en faveur de cette solution, v. Suzanne CARVAL, *op. cit.*, spéc. n° 323, p. 366.
[1479] V. en ce sens, Daniel FASQUELLE et Rodolphe MESA, « La sanction de la concurrence déloyale et du parasitisme et le rapport Catala », chron., préc., spéc. 2667.
[1480] Rapport d'information n° 558 préc., recommandation n° 24 préc. : « *Autoriser les dommages et intérêts punitifs en cas de fautes lucratives dans certains contentieux spécialisés, versés par priorité à la victime et, pour une part définie par le juge, à un fonds d'indemnisation ou, à défaut, au Trésor public* ». – Sur les différents procédés d'affectation, v. Suzanne CARVAL, *op. cit.*, spéc. n° 322, p. 364 et s. (l'auteur propose plusieurs solutions : les tribunaux pourraient accepter de donner acte à ceux qui en font la demande, de leur intention de donner le produit de la condamnation à une œuvre de bienfaisance. L'affectation des sommes peut également être réalisée de façon contraignante. Rien n'empêche en effet le législateur de prévoir que tout ou partie de la condamnation profitera à l'État ou à des organismes d'utilité publique ou de permettre au juge d'exiger du demandeur qu'il engage les sommes attribuées dans une opération ou un programme de travail, notamment quand le demandeur est une association).
[1481] Proposition de loi portant réforme du droit de la responsabilité civile, proposition préc., proposition d'article 1386-25 du C. civ. : les dommages-intérêts punitifs « *seront versés à la victime et, dans une proportion que le juge déterminera, à un fonds d'indemnisation ou au Trésor public* » .
[1482] En ce sens, v. Philippe LE TOURNEAU, *Droit de la responsabilité et des contrats, op. cit.*, spéc. n° 92, pp. 49-50. – V. dans un sens proche, en matière de dommages corporels, Christophe RADE, « Responsabilité et solidarité : proposition pour nouvelle architecture », *D.* 2003, chron., p. 2247 et s.

contenue dans l'article L. 113-2 du Code des assurances qui dispose que : « *l'assurance ne répond pas, nonobstant toute convention contraire, des pertes et dommages provenant d'une faute intentionnelle ou dolosive de l'assuré* » [1483]. L'exclusion de l'assurance des dommages et intérêts compensatoires dans le cas où une faute intentionnelle a été commise [1484] commande, *a fortiori,* d'adopter la même position s'agissant des dommages-intérêts punitifs [1485]. C'est d'ailleurs ce qu'a proposé le projet CATALA [1486] L'opportunité de cette solution se confirme tout particulièrement en cas de lucrative [1487]. Comme le souligne clairement le professeur Geneviève VINEY, priver l'auteur de la faute lucrative du bénéfice de l'assurance est « *indispensable pour donner à cette condamnation la portée punitive* » [1488] et que la peine privée puisse « *conserver toute sa vertu dissuasive* » [1489]. En effet, il est nécessaire que l'auteur de la faute assume le poids de l'indemnité à laquelle il est condamné. À défaut, il pourrait continuer de profiter des conséquences de sa faute lucrative et tout effet comminatoire serait totalement anéanti. Toutefois, cette solution doit être entourée de certaines garanties, en particulier, le législateur doit veiller à ce que la fixation du montant des dommages-intérêts punitifs soit soumise au respect d'un impératif de pondération [1490].

487. Encadrement du juge. L'octroi de dommages-intérêts punitifs devrait être subordonné à l'obligation pour les juges du fond de motiver leur décision de sanction. C'est en ce sens que le projet CATALA s'est prononcé [1491], tout comme la proposition de loi de 2010 [1492]. Cette exigence est en effet indispensable pour assurer la protection des justiciables ainsi que la bonne mise en œuvre de la peine privée [1493]. Le contrôle opéré par la Cour de cassation permettra ainsi de garantir que « *la peine privée soit appliquée conformément aux*

[1483] V. Geneviève VINEY et Patrice JOURDAIN, *Les effets de la responsabilité, op. cit.,* spéc. n° 365 et s., p. 649 et s.
[1484] V. par ex. Muriel FABRE-MAGNAN, *Responsabilité civile et quasi-contrats, op. cit.,* spéc. p. 95.
[1485] V. en ce sens, Suzanne CARVAL, *op. cit.,* spéc. n° 325, p. 367. – Si cette solution relève du bon sens, la solution n'est toutefois pas automatiquement admise. Aux États-Unis, par exemple, les États ont adopté des positions très contrastées. Suzanne CARVAL rapporte à ce titre que vingt-et-un États sont favorables à l'assurance contre huit qui manifestent leur opposition, dix n'ont pas tranché la question et six prévoient une assurance possible dans les hypothèses les dommages-intérêts punitifs sont prononcés à l'encontre d'un responsable du fait d'autrui (*ibid*., spéc. n° 326, p. 368).
[1486] V. projet CATALA préc., selon l'art. 1371 du projet : « *Les dommages-intérêts punitifs ne sont pas assurables* ».
[1487] V. not. Patrice JOURDAIN, « Rapport introductif », rapport préc., spéc. n° 10, p. 5.
[1488] En ce sens, v. Geneviève VINEY, « De la responsabilité civile (articles 1340 à 1386) : exposé des motifs », préc., spéc. p. 148.
[1489] Suzanne CARVAL, *La responsabilité civile dans sa fonction de peine privée, op. cit.*, spéc. n° 327, p. 371.
[1490] Sur cet impératif de pondération, v. *infra* n° 489.
[1491] V. projet CATALA préc., art. 1371 : « *La décision du juge d'octroyer de tels dommages-intérêts doit être spécialement motivée* ».
[1492] Proposition de loi portant réforme du droit de la responsabilité civile, proposition préc., proposition d'article 1386-25 du C. civ : « *le juge peut condamner, par décision motivée, l'auteur du dommage* […] *à des dommages et intérêts punitifs* ».
[1493] Suzanne CARVAL, *op. cit.*, spéc. n° 317, pp. 360-361.

vœux du législateur, et non de façon anarchique et fantaisiste »[1494]. À cette fin, il serait souhaitable que la Haute juridiction vérifie que les éléments pris en compte par les premiers juges dans le calcul de la réparation respectent fidèlement l'esprit des textes instituant des peines privées. Ce pouvoir de contrôle aurait notamment pour effet de lui permettre de censurer une décision qui ne prononcerait qu'une peine symbolique alors même que la faute aurait généré d'importants bénéfices au profit de son auteur ou bien au contraire, une décision qui ne ferait que calquer une peine déjà prononcée dans une espèce similaire en ignorant les particularités de l'espèce. En effet, si l'on ne peut nier que la prise en compte des décisions antérieures favorise la cohérence au sein de la jurisprudence, elle ne doit toutefois pas inciter les juges à abandonner totalement leur liberté d'appréciation du montant de la sanction dans la mesure où la peine privée, à l'instar des dommages et intérêts compensatoires, doit être appréciée *in concreto* [1495].

488. La question de l'évaluation des dommages et intérêts punitifs. Le projet CATALA ne se prononce nullement sur les modalités de calcul destinées à fixer le montant des dommages-intérêts punitifs, se limitant à énoncer que « *leur montant doit être distingué de celui des autres dommages-intérêts accordés à la victime* » [1496]. Or, un tel silence est regrettable puisqu'il est source d'insécurité juridique. En effet, s'il semble nécessaire de laisser une certaine liberté d'appréciation aux juges afin qu'il puisse prononcer une sanction adaptée à l'espèce considérée, l'absence de toutes directives à l'attention des juges leur confère un pouvoir trop large qui risque de donner lieu à des décisions imprévisibles, voire très contrastées. Une autre solution plus rigoureuse pourrait consister à fixer un montant égal à un multiple du profit réalisé sur le modèle de nombreux droits étrangers [1497] qui consacrent des dommages-intérêts multiples [1498]. Toutefois, cette proposition reste insuffisante puisqu'elle reste étroitement liée au préjudice subi par la victime. Or, il est des cas où les bénéfices retirés seront nettement supérieurs au dommage qui en découle. Dans ce cas de

[1494] Suzanne CARVAL, *ibid*., spéc. n° 317, p. 360.
[1495] V. en ce sens, Suzanne CARVAL, *ib., loc. cit.*
[1496] V. le nouvel article 1371 du Code civil proposé.
[1497] Aux États-Unis, par exemple, le paragraphe 2 de la section 284 du Titre 35 du Code des États-Unis sanctionnant la contrefaçon de brevets prévoit que le tribunal peut alourdir le montant de la réparation jusqu'à trois fois celui des dommages et intérêts compensatoires (v. sur ce point, Pierre VERON et Stanislas ROUX-VAILLARD, « Les dommages-intérêts pour contrefaçon de brevet en droit américain », *RLDI* mars 2006, Étude 425, p. 67 et s.).
[1498] Sur la notion de dommages-intérêts multiples, v. Christelle COUTANT-LAPALUS, *Le principe de la réparation intégrale en droit privé*, *op. cit.*, spéc. n° 468, p. 395 (« *Les dommages-intérêts multiples peuvent se définir comme une mesure visant à réprimer l'auteur du dommage, tout en restant proportionnée au montant du préjudice subi par la victime* »). – V. ég. Juliette MEADEL, « Faut-il introduire la faute lucrative en droit français ? », art. préc., spéc. n° 28, p. 12 (« *Les dommages-intérêts multiples peuvent se définir comme une mesure visant à réparer le préjudice subi par la victime qui a droit à la restitution des profits illégitimement perçus par l'auteur de la faute. Ainsi, une fois l'étendue du préjudice déterminée, son montant est multiplié par un coefficient fixé par le législateur et variant selon le montant des bénéfices illicites. Le résultat est attribué à la victime de la faute lucrative* »).

figure, cette solution ne permettra pas de neutraliser totalement les profits réalisés, laissant ainsi subsister les montants supérieurs à la référence retenue. Cette même critique peut être adressée à l'encontre des propositions énoncées dans le rapport d'information de 2009 qui propose de calculer le montant des dommages-intérêts punitifs en considération de celui des intérêts compensatoires [1499] et dans la proposition de loi de 2010 qui suggère que le montant des dommages-intérêts punitifs « *ne peut dépasser le double du montant des dommages et intérêts compensatoires* » [1500]. Si toutes ces solutions présentent l'avantage de la prévisibilité par rapport à la méthode proposée par le projet CATALA, elles apparaissent néanmoins trop rigides. Leur application systématique risque d'entraver l'appréciation des juges et les empêcher de rendre des décisions pleinement adaptées aux faits considérés. En définitive, un système de calcul intermédiaire s'insérant entre l'inflexibilité et le trop permissif semble dès lors s'imposer. Dans cette optique, le texte pourrait fixer un plafond [1501] et indiquer, à l'instar de la méthode d'évaluation utilisée par les autorités de la concurrence [1502], plusieurs paramètres pouvant être pris en compte dans l'appréciation du préjudice, à savoir : la gravité de la faute, les profits réalisés, l'ampleur de la réparation, … Si cette méthode venait à être retenue, elle impliquerait inévitablement un changement d'orientation quant au mode d'évaluation actuel et répondrait aux vœux précédemment formulés. Retenir cette solution aurait en effet deux conséquences : d'une part, les juges du fond seraient tenus de motiver leurs décisions et d'autre part, il appartiendrait à la Cour de cassation de s'assurer que les conditions de déclenchement de la responsabilité sont bien réunies et d'examiner les éléments pris en compte par les juges du fond dans le chiffrage de la peine [1503].

[1499] « *le montant serait fixé en fonction de celui des dommages et intérêts compensatoires* » (rapport d'information n° 558 préc., spéc. recommandation n° 24 préc.).

[1500] Proposition de loi portant réforme du droit de la responsabilité civile, proposition préc., proposition d'article 1386-25 du C. civ.

[1501] En faveur d'une prédétermination du montant de la peine par le législateur, v. not. Suzanne CARVAL, *La responsabilité civile dans sa fonction de peine privée*, *op. cit.*, spéc. n° 314, p. 355. – Stéphane PIEDELIEVRE, « Les dommages-intérêts punitifs : une solution d'avenir ? », *in* colloque Chambéry préc., étude préc., spéc. n° 18, p. 71.

[1502] Art. L. 464-2 C. comm. : Les Autorités de la concurrence prononcent des sanctions pécuniaires « *proportionnées à la gravité des faits reprochés, à l'importance du dommage causé à l'économie, à la situation de l'organisme ou de l'entreprise sanctionné ou du groupe auquel l'entreprise appartient et à l'éventuelle réitération de pratiques prohibées par le présent titre* ». Le texte ajoute que lorsque le contrevenant n'est pas une entreprise, le montant maximum de la sanction est de 3 millions d'euros et lorsque c'est une entreprise, le montant maximum de la sanction est de « *10 % du montant du chiffre d'affaires mondial hors taxes le plus élevé réalisé au cours d'un des exercices clos depuis l'exercice précédant celui au cours duquel les pratiques ont été mises en œuvre* ». – Comp. art. 1621 C. civ. du Québec : « *Lorsque la loi prévoit des dommages-intérêts punitifs, ceux-ci ne peuvent excéder en valeur, ce qui est suffisant pour assurer leur fonction préventive. Ils s'apprécient en tenant compte de toutes les circonstances appropriées, notamment de la gravité de la faute du débiteur, de sa situation patrimoniale ou de l'étendue de la réparation à laquelle il est déjà tenu envers le créancier, ainsi que, le cas échéant, du fait que la prise en charge du paiement réparateur est, en tout ou partie, assumée par un tiers* ».

[1503] Sur ce point, v. Suzanne CARVAL, *La responsabilité civile dans sa fonction de peine privée*, *op. cit.*, spéc. n° 317, pp. 360-361. – Stéphane PIEDELIEVRE, « Les dommages-intérêts punitifs : une solution d'avenir ? », *in* colloque Chambéry préc., étude préc., spéc. n° 19, p. 71.

489. L'impératif de modération du montant de la réparation. Quelle que soit la méthode finalement retenue, il est tout à fait essentiel, si le législateur venait à consacrer officiellement les dommages-intérêts punitifs, que leur montant soit emprunt de modération et ce, afin d'éviter les dérives du système américain qui ont pu être observées à l'occasion de décisions allouant des sommes exorbitantes aux victimes [1504]. Dans cette optique, il est indispensable que le montant de l'indemnité octroyée respecte le principe de proportionnalité et qu'il soit fixé en considération « *de la capacité financière du fautif ainsi que, le cas échéant, des profits qu'il a pu en retirer* » [1505]. Dans une perspective internationale, cette exigence est opportune puisqu'elle permettrait d'échapper aux risques de censure de la part des juridictions communautaires. Le règlement n° 864/2007 du 11 juillet 2007 sur la loi applicable aux obligations non contractuelles autorise en effet les tribunaux des États membres à considérer une disposition de la loi désignée par le règlement comme contraire à l'ordre public du for et aux lois de police si l'application de cette disposition conduit à l'octroi de dommages-intérêts punitifs excessifs [1506]. Interprétée *a contrario*, cette disposition signifie que tout montant fixé de façon raisonnable ne devrait pas être jugé contraire à l'ordre public du for dans le pays où la reconnaissance de la décision est demandée [1507].

490. Question du cumul avec la sanction pénale. La coexistence de la fonction répressive de la responsabilité civile et de la responsabilité pénale conduit inévitablement à envisager la question du cumul entre ces deux types d'instruments répressifs. *A priori*, notre droit positif apparaît ne montrer aucune résistance à l'idée d'un possible cumul. La condamnation du responsable à réparer le dommage provoqué par sa faute ne s'oppose pas à ce qu'il soit également sanctionné au titre de la violation de la loi pénale et inversement [1508]. Ce cumul est rendu possible en raison de la finalité propre que chacune de ces sanctions poursuit [1509]. Toutefois, comme le souligne le professeur Suzanne CARVAL, cette

[1504] V. en ce sens, *BMW North America Inc. c/ Gore*, 517 *U.S.* 559 (May 20,1996) (la Cour Suprême des États-Unis avait, pour la première fois, déclaré inconstitutionnels les dommages-intérêts punitifs fixés en raison de leur montant jugé excessif et avait conduit la Cour à conclure à la violation du *due process of law*).

[1505] Philippe LE TOURNEAU, *Droit de la responsabilité et des contrats*, *op. cit.*, spéc. n° 45, p. 31.

[1506] Considérant 32 : « *l'application d'une disposition de la loi désignée par le présent règlement qui conduirait à l'octroi de dommages et intérêts exemplaires ou punitifs non compensatoires excessifs peut être considérée comme contraire à l'ordre public du for, compte tenu des circonstances de l'espèce et de l'ordre juridique de l'État membre de la juridiction saisie* ».

[1507] Sur l'absence de contrariété des dommages-intérêts punitifs à l'ordre public international, v. Cass. civ. 1re, 1er déc. 2010, pourvoi n° W09-13.303.

[1508] V. Geneviève VINEY, *Introduction à la responsabilité civile*, 3e éd., L.G.D.J., coll. Traité de droit civil, 2008, spéc. p. 187 et s.

[1509] Alexis JAULT, *La notion de peine privée , op. cit.*, spéc. nos 400-401, p. 261 et s. et note 3, p. 258 (« *En raison de leurs finalités différentes, les deux pénalités ne s'excluent pas mutuellement et peuvent, au contraire, se compléter. En effet, la nécessaire protection de la société peut et doit s'accompagner d'une protection des intérêts particuliers susceptibles d'être lésés par une infraction* ». […] « *si toutes deux ont pour objet de sanctionner un comportement, l'une d'entre elles, la peine privée, assure le respect de " l'ordre juridique privé ", tandis que la seconde, la peine publique, vise à protéger toute atteinte à la cohésion* sociale »). – Pour des exemples de cumul, v. Alexis JAULT, *La notion de peine privée , op. cit.*, spéc. p. 260.

superposition risque, dans certaines hypothèses, d'exposer le responsable à de lourdes sanctions qu'il ne pourra pas assumer financièrement. Pour éviter une telle conséquence, le recours à la peine privée doit s'opérer de façon raisonnable, en privilégiant la substitution des sanctions plutôt que leur juxtaposition [1510]. Si toutefois un tel cumul s'imposait, il serait intéressant que le législateur édicte une règle consistant à limiter le montant global des sanctions prononcées au montant de la sanction la plus élevée à laquelle il s'expose, telle que l'a fixée le Conseil Constitutionnel en cas de cumul de sanctions pénale et administrative en matière d'infractions boursière [1511].

B. L'OPPORTUNITE DE CONSACRER UNE ACTION DE GROUPE

491. Le réveil d'anciennes propositions. L'importance de faciliter l'action en réparation des victimes de faute lucrative conduit à s'interroger quant à l'opportunité de consacrer en droit interne une action de groupe. S'il n'existe actuellement aucun équivalent de la *class action* en droit français, l'idée de son introduire n'est toutefois pas nouvelle et a vu le jour à partir des années quatre-vingt à travers diverses propositions [1512]. En septembre 1983, la Commission sur le règlement des litiges de la consommation, présidée par le professeur Jean CALAIS-AULOY, avait rendu un rapport dans lequel était exposé le projet d'instituer une action de groupe. Deux ans plus tard, ce projet avait été repris dans une proposition à l'initiative de la Commission de refonte du droit de la consommation, également présidée par Jean CALAIS-AULOY ainsi que dans un projet de portée plus générale, non limité au droit de la consommation, rédigé par Francis CABALLERO. Aucune de ces propositions n'est toutefois parvenue à voir le jour [1513].

[1510] Suzanne CARVAL, *La responsabilité civile dans sa fonction de peine privée*, *op. cit.*, spéc. n° 333, p. 376.

[1511] Pour une solution identique adoptée en matière d'infractions boursières, en cas de cumul de sanctions adminstratives et pénales, v. Cons. const., DC n° 89-260 du 28 juillet 1989, J.O. du 1er août 1989, p. 9676 et s., *Rec. const.*, p. 71, spéc. considérant 22, p. 9678 : « *Considérant que la possibilité n'est pas moins reconnue à la Commission des opérations de bourses de valeurs de prononcer une sanction pécuniaire* […] *qui est susceptible de se cumuler avec des sanctions pénales prononcées en raison des mêmes faits* […] *si l'éventualité d'une double procédure peut ainsi conduire à un cumul de sanctions, le principe de proportionnalité implique, qu'en tout état de cause, le montant global des sanctions éventuellement prononcées ne dépasse pas le montant le plus élevé de l'une des sanctions encourues* ».

[1512] Pour un aperçu de l'action de groupe en Europe, v. Jérôme FRANCK, « Action de groupe : les initiatives européennes en droit interne et en droit communautaire », in « Les class actions " devant le juge français : rêve ou cauchemar ? – Colloque Paris, 18 nov. 2004 », *LPA* 10 juin 2005, n° 115, p. 19 et s.

[1513] Pour un descriptif détaillé du contenu de ces propositions destinées à introduire une action de groupe, v. not. Louis BORE, *La défense des intérêts collectifs par les associations devant les juridictions administratives et judiciaires*, (préf. Geneviève VINEY), tome 278, L.G.D.J., coll. *Bibl. dr. privé*, 1997, spéc. n° 403 et s., p. 401 et s. (sur le projet CALAIS-AULOIS, v. *ibidem.*, spéc. nos 404-408, pp. 402-407 et sur le projet CABALLERO, v. *ibid.*, spéc. nos 409-414 , pp. 407- 411). – V. ég. Francis CABALLERO, « Plaidons par Procureur ! : De l'archaïsme procédural à l'action de groupe », *RTD civ.* 1985, p. 247 et s., spéc. n° 27 et s., p. 272 et s.

492. Une consécration controversée. La reconnaissance officielle d'une action de groupe a soulevé de nombreuses critiques. Ses opposants ont soutenu qu'une telle reconnaissance contreviendrait aux principes fondamentaux du droit processuel français et notamment à la prohibition des arrêts de règlement [1514], à la relativité de la chose jugée, à la règle selon laquelle « Nul ne plaide par procureur » [1515], autorisant les seules personnes mandatées à agir pour défendre les intérêts d'autrui, ou encore au respect du contradictoire et des droits de la défense [1516]. Outre ces obstacles juridiques, ont été notamment dénoncés les honoraires des avocats, considérés comme disproportionnés par rapport aux sommes perçues par les membres du groupe. Si l'on ne peut ignorer ces critiques, il a été largement démontré qu'elles ne sont pas insurmontables [1517]. Aussi, plutôt que de s'obstiner à maintenir un rejet absolu de ce type d'action, il serait préférable de réfléchir au contexte dans lequel elles

[1514] Art. 5 C. civil.

[1515] Pour une critique de cette règle, v. Francis CABALLERO, art. préc., spéc. n[os] 4-13, pp. 251-261 (la considérant comme « [a]*rchaïque, inutile et discriminatoire* » (*id.*, spéc. n° 10, p. 259)).

[1516] Sur ces critiques, v. Marie-Anne FRISON-ROCHE, « Les résistances mécaniques du système français à accueillir la *class action* : obstacles et compatibilités », *in* colloque Paris préc., *LPA* 10 juin 2005, n° 115, p. 22 et s. – Séverine CABRILLAC, « Pour l'introduction de la class action en droit français », *LPA* 18 août 2006, n° 165, p. 4 et s.

[1517] Selon Louis BORE, « *il n'y a aucune atteinte au principe d'autorité relative de la chose jugée puisque tous les membres du groupe représenté sont considérés comme étant partie à l'instance* » (*La défense des intérêts collectifs par les associations devant les juridictions administratives et judiciaires, op. cit.*, spéc. n° 419, p. 414 et s.). Quant à la critique selon laquelle l'action de groupe porterait atteinte au libre exercice du droit d'action en justice, il répond très justement que « [s]*ur le plan pratique,* […] *lorsque, dans une action de groupe, les droits en question sont d'une valeur patrimoniale minime, leurs titulaires n'auraient de toutes façons pas engagé les frais d'un procès pour les défendre* » et précise que « *cette barrière constitutionnelle, qui assure la primauté de l'intérêt individuel sur le collectif, ne constitue pas un obstacle insurmontable. On peut imaginer une action de groupe plus souple et plus ouverte que les modèles américains et québécois, dans laquelle les membres du groupe pourraient se retirer* » (*ibid.*, spéc. n° 419, p. 415). – V. ég. Séverine CABRILLAC, « Pour l'introduction de la class action en droit français, art. préc., spéc. n° 5 et s., p. 6 et s. – Marie-Anne FRISON-ROCHE énonce à juste titre, s'agissant des arrêts de règlement, que le jugement obtenu par *class action* « *n'apparaît tout simplement pas comme un arrêt de règlement* » […] dans la mesure où « *il ne joue pas pour les situations à venir, il est très classiquement un acte juridictionnel qui apure le passé* […] *en ayant d'effet que sur des situations déjà passées* » (« Les résistances mécaniques du système juridique français à accueillir la class action : obstacles et compatibilités », art. préc., spéc. n° 14, p. 24. – Sur ce point, v. ég. Michel VERPEAUX, « L'action de groupe est-elle soluble dans la Constitution ? », *D.* 2007, point de vue, pp. 258-259, spéc. p. 259 : « *la décision relative à cette action collective, aussi générale soit-elle, ne vise que des situations passées et ne saurait en conséquence avoir des effets pour l'avenir. Le jugement relatif à une " class action à la française " ne saurait être assimilé à un arrêt de règlement* ») ; Marie-Anne FRISON-ROCHE ajoute que « [s]*i on a pu douter de la compatibilité entre relativité de la chose jugée et class action, c'est parce que l'on confond souvent autorité de chose jugée et pouvoir de contrainte du jugement. Le jugement obtenu par class action contraint le défendeur à l'égard de toutes les personnes de la classe, mais ne supprime pas le droit individuel d'action, ce qui est le seul objet de la chose juge* » (art. préc. spéc. n° 18, p. 24) ; Marie-Anne FRISON-ROCHE ajoute enfin que pour qu'une *vraie class action* soit consacrée par le législateur, c'est-à-dire sans mandat, elle propose, de façon opportune, que celle nouvelle loi se fonde « *expressément sur la théorie de l'accès au droit et au juge et prévoir un droit de sortie, afin que la liberté individuelle du membre de la classe ne soit pas froissée* » (art. préc., spéc. n° 30, p. 26). – S'agissant des droits de la défense, Michel VERPEAUX souligne que ces derniers ne sont pas bafoués s'il existe « *une grande homogénéité dans la situation de fait et de droit des membres du groupe* » (« L'action de groupe est-elle soluble dans la Constitution ? », point de vue préc., spéc. p. 259). – V. ég. Jean-David BENICHOUX et Youssef KHAYAT, « La relativité de l'incompatibilité de la *class action* avec le système juridique français », *in* Daniel MAINGUY (sous la dir.), « L'introduction en droit français des class actions », *LPA* 22 déc. 2005, n° 254, p. 6 et s., spéc. p. 19 et s. – Serge GUINCHARD, « Une *class action* à la française ? », *D.* 2005, doctr., p. 2180 et s. – Reprenant brièvement l'ensemble des arguments précités, Dimitri HOUTCIEFF conclut qu'« [i]*l faut s'y résoudre, il n'y a pas d'exception française en matière de class action : aucun empêchement dirimant n'interdit la création d'une action de groupe en droit français* » (« Rapport de synthèse », *in* colloque Paris préc., *LPA* 10 juin 2005, n° 115, p. 42 et s., spéc. p. 44-45).

pourraient opportunément s'insérer. Nous verrons que les dommages de masse, comme ceux provoqués par le *spamming*, sont devenus désormais une réalité incontestable et nécessitent leur prise en compte par le droit français (1.). Cette réalité conduit à rechercher des solutions permettant de répondre à ce problème spécifique. Pour cela, certains droits étrangers ont déjà eu l'occasion de se mesurer à ce phénomène et à ce titre, peuvent être une source d'inspiration intéressante. En particulier, le succès de la *class action* en droit étranger, et notamment aux États-Unis, nous invitera à lui porter une attention toute particulière (2.) et nous conduira, en dernière analyse, à réfléchir à titre prospectif aux contours qu'elle pourrait prendre si une institution semblable venait à être consacrée en droit français (3.).

1. La nécessaire prise en compte des dommages de masse par le droit français

493. L'importance des dommages de masse. Les capacités offertes par le réseau permettent notamment de transmettre simultanément une même information à des milliers, voire des millions de personnes. La pratique du *spamming* illustre parfaitement l'exploitation de telles capacités de communication. Mais dès lors que cette communication à grande échelle cause un dommage, ses effets ont également une forte ampleur. Si nous reprenons l'exemple du *spamming*, l'envoi de *spams*, fait générateur unique, est à l'origine d'une atteinte diffuse qui consiste en la somme des dommages subis individuellement par chacun des destinataires. Ce préjudice de grande envergure n'est pas sans rappeler la notion de « dommages de masse ». En effet, ce type de dommages, caractérisé par son aspect quantitatif, correspond à une situation dommageable d'une ampleur exceptionnelle qui procède d'un fait ou d'une activité imputable au même auteur et qui atteint simultanément un grand nombre de victimes [1518]. Ces dommages de masse laissent ainsi apparaître un déséquilibre entre les pouvoirs des victimes et ceux de l'auteur du dommage : tandis que les premières, isolées, ne disposent pas de moyens juridiques pour se défendre car leur dommage est difficilement réparable, le second qui a peu de risque d'être poursuivi par ces victimes peut poursuivre ses activités sans être inquiété.

494. L'expérience américaine comme source d'inspiration. Au risque de se heurter à certaines critiques dénonçant un risque de « dérive américaine » [1519], il convient de

[1518] Sur cette notion de dommages de masse, v. Anne GUEGAN-LECUYER, *Dommages de masse et responsabilité civile*, (préf. Patrice JOURDAIN, avant-propos Geneviève VINEY), tome 472, L.G.D.J., coll. *Bibl. dr. privé*, 2006, spéc. n[os] 46-51, p. 53 et s.

[1519] Laurence ENGEL, « Vers une nouvelle approche de la responsabilité : Le droit français face à la dérive américaine », *in Qui est responsable ? Qui est coupable ?, Esprit* juin 1993, p. 5 et s. – On retrouve cette même crainte du « *phantasme de l'américanisation* », en matière de *class action* (v. *infra* : n° 495 et s.), pour reprendre

souligner que cette notion n'est pas sans évoquer celle des « *mass torts* » existant en droit américain [1520]. Loin de constituer une menace en ce qu'elle favoriserait une américanisation de notre droit de la responsabilité, ce rapprochement est davantage destiné à aider les juristes français à identifier une réalité désormais indéniable. Précurseurs en la matière, les praticiens américains ont eu le mérite de traiter le problème de front et de mettre en évidence un phénomène dont l'existence est bien réelle puis de rechercher des solutions adéquates. Pour apaiser les plus inquiets, il ne s'agit pas de transposer aveuglément et de façon mécanique ce qui existe en droit américain mais plutôt, à partir d'une expérience déjà largement éprouvée, de s'en inspirer afin de mieux appréhender les répercussions que pourrait avoir la reconnaissance d'un phénomène similaire sur notre droit de la responsabilité civile [1521].

2. L'opportunité de recourir à la *class action* en cas de dommages de masse

495. La nécessité de faciliter l'action des victimes de dommages de masse. Dans l'hypothèse des dommages de masse, le préjudice subi individuellement est infime. Si l'on prend l'exemple du *spamming*, les millions voire les milliers d'internautes victimes du même « spammeur » ne subissent en réalité qu'une simple gêne puisque chacun d'entre eux ne recevra qu'un seul *spam* [1522]. Dans ces circonstances, il existe peu de chances pour que les victimes entreprennent une action qui risque d'être longue et coûteuse, ce qui laisse ainsi le « spammeur » poursuivre ses activités en toute quiétude. Et même si elles venaient à engager une telle action, elles risquent de se heurter au refus des juges d'indemniser ce type de dommage en raison de son caractère négligeable [1523]. Dans une optique de lutte optimale contre le *spamming*, cette situation ne peut perdurer et il convient de donner à l'ensemble des « spammés » les moyens juridiques de se défendre efficacement contre cette pratique. Face à l'impasse devant laquelle se trouve cette catégorie de victimes, et à la volonté de trouver une alternative à l'action pénale considérée comme trop rigide et insuffisante pour combler les lacunes du droit de la responsabilité, se pose donc avec acuité la question d'une rénovation du droit de la responsabilité civile destinée à offrir une action adaptée à l'ampleur et à la

l'expression de Dimitri HOUTCIEFF, et qui attire l'attention sur le fait que « [s]*i la dérive est un risque bien réel, il ne doit pas dégénéré en fantasmagorie* » (« Rapport de synthèse », *in* colloque Paris préc., rapport préc., spéc. pp. 45-46).

[1520] Sur cette notion de *mass torts* et son influence en matière de responsabilité civile, v. Anne GUEGAN-LECUYER, *Dommages de masse et responsabilité civile, op. cit.*, n° 54-56 , p. 59 et s.

[1521] V. ég. en ce sens, Anne GUEGAN-LECUYER, *Dommages de masse et responsabilité civile, ibid.*, spéc. n° 59, p. 68 (« *Il s'agit plutôt de permettre, avec quelques dizaines d'années de retard, l'identification d'un phénomène dommageable dont la réalité est certaine et qui doit permettre de mieux cerner ses influences sur les mécanismes de responsabilité civile* »).

[1522] Plus précisément, cette gêne ne résulte pas de la réception de ce seul message mais de multiples messages déjà reçus auparavant en provenance de différents « spammeurs ».

[1523] Sur ce refus des juges, v. *supra* : n° 486.

particularité de ce type de dommage. Plus exactement, il convient de s'interroger sur une possible introduction d'une action de groupe en droit français, spécifiquement lorsque le préjudice individuel est quantitativement insignifiant. La question de l'introduction d'une action de groupe en droit français requiert une analyse des expériences étrangères afin de saisir leur mécanisme et de proposer, le cas échéant, des aménagements destinés à faciliter son admission en droit français.

496. L'exemple de la *class action* américaine. D'origine anglo-saxonne, l'exemple américain constitue toutefois le modèle emblématique de la *class action* qui a inspiré d'autres pays étrangers et sur lequel nous appuierons nos développements. La action peut être définie comme celle « *introduite par un représentant pour le compte de toute une classe de personnes ayant des droits identiques ou similaires qui aboutit au prononcé d'un jugement ayant autorité de chose jugée à l'égard de tous les membres de la classe* » [1524]. L'objectif de cette action est de favoriser l'accès à la justice à un groupe très important de personnes victimes de dommages de masse et de faire ainsi gagner du temps aux tribunaux en jugeant en une seule fois un litige qui aurait pu donner lieu à de multiples actions individuelles. Introduite en 1938 par la règle 23 du Code de procédure civile fédérale et calquée dans la plupart des états fédérés, son véritable essor débuta en 1966, date à laquelle cette règle fut modifiée afin d'encourager l'expansion de cette action.

497. Le déroulement de la *class action*. Schématiquement, la *class action* est soumise à une procédure préalable de certification qui consiste pour le juge à contrôler la recevabilité de l'action au regard des conditions posées par la règle 23 précitée [1525]. Pour cela, le juge doit apprécier l'opportunité d'une telle action en recherchant si elle se présente comme la plus adaptée et la plus efficace pour régler le litige considéré. Tel sera le cas, par exemple, s'il existe des risques à engager des actions distinctes qui pourraient aboutir à des décisions contradictoires à l'égard des membres du groupe [1526] ou si les points de droit ou de fait communs au groupe prévalent sur tout autre point qui n'intéresserait individuellement que certains membres du groupe [1527]. Lors de cette première opération de vérification, les

[1524] Louis BORE, *La défense des intérêts collectifs par les associations devant les juridictions administratives et judiciaires*, *op. cit.*, spéc. n° 353, p. 359.
[1525] Pour une description détaillée de la règle 23, v. Louis BORE, *ibidem.*, spéc. n° 354 et s., p. 360 et s. – Francis CABALLERO, « Plaidons par Procureur ! : De l'archaïsme procédural à l'action de groupe », doctr. préc., spéc. n° 15 et s., p. 262 et s. – Florence LAROCHE-GISSEROT, « Les *class actions* américaines », *in* colloque Paris préc., *LPA* 10 juin 2005, n° 115, p. 7 et s. – Comp. avec le recours collectif québécois, v. not. Louis BORE, *ibid.*, spéc. n° 373 et s., p. 380 et s. – Anne GUEGAN-LECUYER, *Dommages de masse et responsabilité civile*, *op. cit.*, n° 361 et s., p. 419 et s. – Pierre-Claude LAFOND, « Le recours collectif et le juge Québécois : De l'inquiétude à la sérénité », *in* colloque Paris préc., *LPA* 10 juin 2005, n° 115, p. 11 et s.
[1526] Louis BORE, *ibid.*, spéc. n° 358, p. 362.
[1527] Louis BORE, *ibid.*, spéc. n° 360, p. 364.

juges jouissent d'un large pouvoir d'appréciation leur permettant ainsi de rendre des jugements « *élaborés " sur mesure* " » [1528]. La procédure de certification conduit également le juge à vérifier la qualité de la personne désignée comme représentant [1529]. Il lui appartient à ce titre de s'assurer d'une part, que l'action envisagée par le représentant soit très proche de celle que les membres auraient entreprise s'ils avaient agi à titre individuel et d'autre part, qu'elle soit fondée sur des points de droit ou de fait communs au groupe qu'il envisage de représenter. Outre le contrôle judiciaire de l'aptitude du représentant à défendre efficacement les intérêts du groupe, les juges américains doivent également vérifier sur les compétences de son avocat. À l'issue de cette procédure de certification, le juge se prononcera sur la recevabilité de la *class action.* Lorsque celle-ci est jugée recevable, une notification est adressée aux membres du groupe [1530] afin que ces derniers aient connaissance de l'existence de cette action [1531]. Une fois informés, ils peuvent choisir de se retirer du groupe ou au contraire d'intervenir dans l'instance (« *opt-out* »). Il s'ensuit que les personnes qui n'auront pas adressé au tribunal un écrit l'informant de leur exclusion du groupe avant une date limite fixée par le juge, seront considérées comme appartenant à ce groupe et la décision s'imposera alors à ces dernières [1532]. S'agissant de l'instance, son déroulement est facilité grâce aux moyens que la règle 23 met à disposition du juge pour appréhender le litige. À ce titre, il peut adapter le champ de l'action en réduisant son objet [1533] ou en fractionnant le groupe selon certaines particularités, notamment la gravité des dommages [1534]. Enfin, lorsque les éléments de preuve produits par le représentant sont jugés probants, ils sont présumés s'appliquer à l'ensemble des membres du groupe. Le tribunal se réunit alors pour juger l'affaire au fond mais le plus souvent, les *class actions* se soldent par une transaction, justifiée notamment par l'importance des condamnations encourues qui encourage fortement le défendeur à transiger. Dans ce cas, la règle 23 impose que la transaction soit notifiée à tous les membres du groupe [1535]. Pour des raisons de sécurité juridique, la transaction n'acquiert force obligatoire qu'après l'autorisation du tribunal [1536], autorisation qui sera

[1528] Louis BORÉ, *ibid.*, spéc. n° 360, p. 368.
[1529] Louis BORE, *ibid.*, spéc. n° 361 et s, p. 368 et s.
[1530] Pour les *class action* en réparation, la règle 23, al. (c) (2) dispose que : « *Le tribunal adresse aux membres du groupe la notification la mieux adaptée aux circonstances, notamment une notification individuelle à tous les membres du groupe qu'un effort raisonnable permet d'identifier* ». En revanche, pour les *class action* déclaratoires ou en injonction, la notification n'est pas obligatoire (v. Louis BORE, *ibid.*, spéc. n° 365, p. 371).
[1531] Sur les modalités de la notification et son contenu, v. Louis BORE, *ibid.*, spéc. n° 367, p. 372.
[1532] Louis BORE, *ibid.*, spéc. n° 366, p. 372.
[1533] À ce titre, Louis BORE cite, à titre d'exemple, l'action en responsabilité : en ce domaine, le juge peut limiter la *class action* à la question de l'existence de la faute ou du fait générateur de responsabilité et renvoyer la question des dommages et des liens de causalité à des actions individuelles engagées par chaque victime (*ibid.*, spéc. n° 369, p. 374).
[1534] Louis BORE, *ibid., loc. cit.*
[1535] Régle 23, al. (e).
[1536] Régle 23, al. (e).

donnée à l'issue d'un contrôle de l'intérêt du groupe afin de s'assurer que le représentant et son conseil ne concluent pas d'accord au détriment du groupe [1537].

498. Une action adaptée aux dommages de masse. Au regard du déroulement de la *class action*, il convient de relever les nombreux avantages que présente cette action. Son intérêt réside avant tout dans la possibilité de trouver une réponse pertinente à l'impunité dont bénéficient injustement les auteurs de dommages de masse. Corrélativement, cette procédure permet notamment de faciliter l'accès à la justice à des « *plaideurs isolés et démunis qui, sans la faculté de se regrouper, renonceraient à faire valoir leurs droits*» [1538]. L'examen judiciaire de la recevabilité de l'action envisagée permet de contrôler en amont son sérieux, de se s'assurer qu'elle s'impose comme la plus adaptée au litige en cause mais également de vérifier le sérieux du représentant. Elle constitue en même temps un moyen de protéger le défendeur contre d'éventuelles actions abusives qui auraient pour effet de compromettre injustement la réputation de ce dernier, et l'exposer à des répercussions économiques graves sur son développement. La souplesse du mécanisme de mise en œuvre de cette action, et notamment la possibilité d'adapter ses contours aux particularités du litige considéré [1539], constitue un avantage incontestable pour assurer le succès de cette action. De même, la possibilité pour le représentant d'agir sans mandat facilite et accélère la mise en œuvre de cette action. Enfin, la faculté pour le magistrat de regrouper, dans une procédure unique, un très grand nombre d'actions individuelles assure une cohérence au sein de la jurisprudence et évite ainsi le risque de décisions contradictoires [1540]. L'ensemble de ces avantages plaide en faveur de la reconnaissance officielle de l'action de groupe, tout particulièrement en matière de *spamming*. En effet, comme nous l'avons souligné dès l'introduction de ces développements, elle permet d'inciter les « spammés » qui ne subiraient qu'un préjudice très minime à se solidariser pour engager une action contre le « spammeur ». Ce regroupement permettrait ainsi de réduire de façon substantielle les cas, beaucoup trop nombreux, où les « spammeurs », agissent sans la crainte de s'exposer à d'éventuelles poursuites.

3. Analyse critique et prospective de l'introduction de la *class action* en droit français

[1537] Pour définir le rôle du juge, Louis BORE parle ainsi de « *gardien du groupe* » (*id.*, spéc. n° 370, p. 376).
[1538] Francis CABALLERO, « Plaidons par Procureur ! De l'archaïsme procédural à l'action de groupe », art. préc., spéc. n° 18, p. 264.
[1539] V. *supra* : n° 497.
[1540] Anne GUEGAN-LECUYER, *Dommages de masse et responsabilité civile, op. cit.*, spéc. n° 360, p. 416-417 et n° 405, p. 440.

499. Sans avoir la prétention de proposer un système créé *ex nihilo*, nous construirons notre réflexion à partir de l'expérience américaine, tout en veillant à limiter les risques de dérives soulevées à son encontre. À partir de cette inspiration étrangère, nous rechercherons comment l'action de groupe pourrait être concrètement envisagée si celle-ci venait à être introduite en France. Trois points seront successivement abordés : le premier correspondant à la phase de certification de l'action de groupe et directement inspiré du modèle américain (a.), le second relatif à l'instance en responsabilité (b.) et enfin le dénouement de l'instance (c.) [1541].

a. La recevabilité de l'action de groupe

500. La certification. À l'instar de la *class action* américaine, l'intervention d'un jugement préalable relatif à la recevabilité de l'action de groupe envisagée apparaîtrait comme un modèle opportun puisque cette phase permettrait de mettre fin en amont à toute action qui serait jugée excessive. Cette idée n'est d'ailleurs pas nouvelle puisque le projet CABALLERO l'envisageait déjà [1542]. La recevabilité de l'action de groupe serait ainsi subordonnée à l'existence de questions communes liant les membres du groupe. Ce contrôle relève du bon sens puisque l'action de groupe n'est pertinente que si elle a vocation à permettre de trancher des questions de fait ou de droit communes aux membres du groupe. Il convient alors de déterminer s'il vaut mieux privilégier une acception large de ces questions conduisant à retenir tout point « similaire », « connexe », « commun » ou, au contraire, adopter une conception restrictive. Si la première solution présente l'avantage d'englober un plus grand nombre de personnes au sein de ce groupe, elle risque d'être source d'interprétations divergentes. Afin d'assurer la sécurité juridique des solutions, il semble donc préférable de consacrer une acception restrictive de cette référence en retenant, par exemple, l'expression « *questions identiques* » proposées par le professeur Sévérine CABRILLAC [1543]. Enfin, comme le souligne très justement le professeur Michel VERPEAUX, la vérification scrupuleuse du juge d'une grande homogénéité entre les situations liant les membres du groupe est essentielle puisqu'elle permettrait de dépasser la critique visant à soutenir une atteinte aux droits de la défense et du contradictoire [1544]. Dans ces conditions en

[1541] Pour une étude d'ensemble, v. not., Séverine CABRILLAC, « Pour l'introduction de la class action en droit français », art. préc.
[1542] V. Louis BORE, *La défense des intérêts collectifs par les associations devant les juridictions administratives et judiciaires*, *op. cit.*, spéc. n° 410 et s., p. 408 et s.
[1543] Séverine CABRILLAC, « Pour l'introduction de la class action en droit français », art. préc., spéc. n° 31, pp. 13-14.
[1544] Michel VERPEAUX, « L'action de groupe est-elle soluble dans la Constitution ? », point de vue préc., spéc. p. 259 .

effet, peu importe que le groupe ne soit pas déterminé à l'avance puisque le défendeur serait actionné en raison des seules questions communes à l'ensemble du groupe. Ainsi, tout en s'écartant de la configuration traditionnellement individuelle de l'action en justice pour se tourner vers une dimension résolument collective de cette dernière, les droits du défendeur s'en trouveraient préserver. L'action de groupe ne pourrait être recevable que si, au surplus, la représentation est conforme aux intérêts à défendre. Cette seconde condition est justifiée par la volonté de protéger les membres en s'assurant de la fiabilité et du sérieux de leur représentant. Elle conduit alors à s'interroger quant à la qualité du requérant et plus précisément, à déterminer si elle doit être limitée au bénéfice des seules associations de consommateurs agréées. Ce choix aurait le mérite d'éviter de rechercher les qualités que devrait réunir le représentant et de dépasser les difficultés d'interprétation qu'elles pourraient susciter. Une telle limitation réduirait néanmoins fortement le champ d'intervention possible des actions de groupe au seul contentieux intéressant le droit de la consommation. Or, cette restriction n'est pas pertinente car elle ôterait à cette action une large part de son intérêt [1545]. En matière de *spamming*, tout particulièrement, on retomberait sur les critiques déjà formulées à propos des loi-anti-*spam* dont le champ d'application est limité aux seuls *spams* à caractère commercial [1546]. Lorsque le tribunal considère l'action recevable, son jugement devra alors préciser la composition du groupe et les juges pourront, à cette occasion, décider de le fractionner en sous-groupes. Le jugement devra également fixer les modalités de la notification de l'avis aux membres du groupe en précisant notamment si elle doit être réalisée de façon individuelle ou collective. Afin d'éviter le risque que certaines personnes ne soient pas informées, la notification individuelle serait préférable, et il conviendrait de réserver la notification collective au seul cas où la première solution se révèle impossible [1547]. S'agissant du contenu de la notification, il serait intéressant de reprendre les dispositions du projet CABALLERO qui permettait aux membres d'avoir une large connaissance de l'action envisagée. À ce titre, l'article 324-5 de ce projet prévoyait que l'avis à notifier aux membres du groupe devait mentionner, à peine de nullité : la juridiction devant laquelle l'action serait introduite, l'identification du représentant et de son conseil, une brève description des éléments de droit et de fait communs aux membres du groupe, le contenu de la décision définissant la composition du groupe, la possibilité de s'exclure du groupe ainsi que toutes autres informations que le juge estime utiles de faire connaître aux membres.

[1545] Sur le rejet d'une action réservée aux associations de consommateurs, v. not. Séverine CABRILLAC, art. préc., spéc. n° 32, p. 14.
[1546] Sur ce point, v. *supra :* n° 300 et s.
[1547] C'est la solution qui a d'ailleurs prévalu dans le projet CABALLERO, v. Louis BORE, *La défense des intérêts collectifs par les associations devant les juridictions administratives et judiciaires*, *op. cit.*, spéc. n° 411, p. 409.

501. La question du mandat. La détermination des conditions relatives à la manifestation de volonté des futurs membres du groupe revient à choisir entre le mécanisme d'*opt-in* ou celui d'*opt-out.* Dans le système de l'*opt-in*, le groupe rassemble seulement les personnes qui ont expressément donné leur accord pour intégrer ce groupe. Le déclenchement de l'action est donc subordonné à un mandat exprès. L'*opt-out* illustre le mécanisme inverse où le groupe est constitué de toutes personnes qui partagent l'intérêt défendu et qui n'ont pas manifesté le souhait d'en sortir. Le choix en faveur de l'un ou l'autre de ces mécanismes dépendra notamment de l'intérêt pratique que le législateur entend donner à cette action. En retenant le mécanisme de l'*opt-in*, la portée pratique de l'action de groupe en serait fortement réduite puisque ce choix aurait pour effet de paralyser certaines des interventions tendant à recourir à cette nouvelle voie en raison de l'absence de mandat. Sur ce point, l'*opt-out* a le mérite de faciliter la mise en œuvre de l'action et répond donc davantage à un souci d'efficacité. Certes, il pourrait lui être reproché le risque de porter atteinte à la liberté individuelle [1548] puisque des individus pourront se retrouver intégrer à un groupe dont ils ne pourront pas se retirer faute de connaître son existence. Ce risque est toutefois moindre dans la mesure où « *d'une part, le juge peut les limiter en intervenant de manière déterminante dans le choix du mode de notification et d'autre part, il existe de nombreux cas dans lesquels les victimes ne se seraient de toute façon pas manifestées de façon individuelle* » [1549]. Par ailleurs, le choix en faveur de l'*opt-out* ne conduit pas les membres du groupe à renoncer à leur d'action individuelle dans la mesure où ils peuvent toujours s'exclure du groupe dès qu'ils le souhaitent pour engager une procédure individuelle [1550]. De même, ils peuvent également agir, après le jugement, pour percevoir les fonds [1551]. L'objectif d'efficacité poursuivi commande, selon nous, de retenir le mécanisme de l'*opt-out* [1552].

[1548] Rappr. Cons. const., DC n° 89-257 du 25 juillet 1989 (J.O. du 28 juillet 1989, p. 9503 et s., *Rec. const*., p. 59) et exigeant que la personne ait « *eu personnellement connaissance* » de l'action engagée par un tiers pour être considérée comme associée à cette dernière (consid. 26).

[1549] Anne GUEGAN-LECUYER, *Dommages de masse et responsabilité civile*, *op. cit.*, spéc. n° 360, p. 416-417.

[1550] Ils pourront toujours décider de se retirer de cette action tant qu'aucun jugement n'aura été prononcé puisqu'une fois rendu, ce dernier aura force obligatoire à l'égard de l'ensemble des membres du groupe. En revanche, si cette action individuelle porte sur des questions autres que celles tranchées dans la décision, ils pourront agir en justice, y compris lorsque le jugement aura été rendu (v. *infra* : n° 503).

[1551] V. Michel VERPEAUX, « L'action de groupe est-elle soluble dans la Constitution ? », point de vue préc., spéc. p. 259.

[1552] En faveur de ce mécanisme, Séverine CABRILLAC, « Pour l'introduction de la class action en droit français », art. préc., spéc. n° 34 et s., p. 15. – Anne GUEGAN-LECUYER, *Dommages de masse et responsabilité civile*, *op. cit.*, spéc. n° 360, p. 416-417. – Michel VERPEAUX, « L'action de groupe est-elle soluble dans la Constitution ? », point de vue préc., spéc. p. 258 (l'action de groupe avec option d'exclusion « *est* […] *de nature à renforcer le droit de tous les justiciables au recours effectif, garanti par l'article 16 de la Déclaration des droits et repris par l'article 13 de la Convention européenne des droits de l'homme, sous le vocable de " droit de recours ". Ce droit, faute de procédure efficace, risque de rester lettre morte* »). – *Contra* Laurent MARTINET et Antoine DE CHASTEL, « Du retour de l'action de groupe et du mythe de Sisyphe », *LPA* 10 mars 2009, n° 49, p. 6 et s. (rejetant l'*opt-out* lorsque certains membres sont indéterminés). – V. ég. Serge GUINCHARD, « Une *class action* à

b. L'action en responsabilité engagée par le représentant

502. Une fois l'action déclarée recevable, il convient de juger au fond les questions communes aux membres du groupe. Rappelons que l'objectif est ici de proposer une réponse pertinente à l'atteinte subi par les « spammés », simples particuliers victimes des envois d'un même « spammeur ». Il est donc essentiel de définir précisément le but de cette action. Comme nous l'avons précédemment expliqué, lorsque le « spammeur » entreprend un envoi massif de *spams*, son objectif est, le plus souvent, de toucher un public le plus large possible de sorte que la gêne occasionnée à chacun des destinataires est tout à fait insignifiante. L'action du représentant ne vise donc pas à obtenir la réparation du dommage mais, en priorité, la cessation pour l'avenir d'un tel comportement afin de s'assurer que le « spammeur » ne renouvellera pas ses agissements [1553]. Dans un tel contexte, l'introduction d'une action en déclaration de responsabilité pour préjudice de masse apparaît opportune [1554] d'autant que sa reconnaissance en serait facilitée dans la mesure où il « *ne semble pas heurter les principes fondamentaux du droit de la responsabilité* » [1555]. En effet, le processus peut être décrit de la façon suivante : à la suite de l'action engagée par le représentant à l'encontre du « spammeur », il appartiendrait au juge saisi de se prononcer sur l'éventuelle responsabilité de ce dernier au regard des règles de droit commun de la responsabilité délictuelle. Pour cela, il aurait pour mission de contrôler l'existence certaine de la faute invoquée, en vérifiant la réalité du profit allégué et l'évaluation qui en aurait été faite par le représentant ainsi que l'existence d'un dommage de masse. Lorsque ces conditions sont réunies, la faute du « spammeur » serait alors établie et l'action aboutirait à un jugement en déclaration de responsabilité de ce dernier pour préjudice de masse. À l'issue de ce jugement, il pourrait ainsi décider de la restitution des profits afin que le « spammeur » soit privé des bénéfices qu'il aura réussi à engranger. Le juge prononcerait alors une mesure de cessation de cette activité illicite pour l'avenir. Ces condamnations devraient être assorties d'astreintes et d'une large publicité de ces peines devrait être organisée afin d'informer toute victime potentielle d'actes similaires à l'origine de cette action de groupe d'en connaître

la française ? », art. préc., spéc. p. 2186 (qui évite la question de l'*opt-out* en proposant que, à la suite du jugement déclaratif de responsabilité, s'ouvre une phase au cours de laquelle l'instance est suspendue et pendant laquelle les victimes du préjudice allégué pourront se manifester, de sorte qu'une fois l'instance reprise, seules les personnes qui se seront fait connaître participeront à cette instance).

[1553] On rejoint ainsi sur ce point le professeur Geneviève VINEY qui, dans ce cas de figure, précise qu'il s'agit « *d'affirmer la responsabilité de l'auteur de la faute, ensuite d'évaluer le profit illicite résultant de celle-ci et d'ordonner sa restitution et enfin d'interdire pour l'avenir la poursuite de l'activité illicite. En revanche, l'attribution des sommes récupérées n'a qu'une importance secondaire* » (« Quelques propositions de réforme du droit de la responsabilité civile », art. préc., spéc. p. 2953).

[1554] V. ég. en ce sens avec une analyse sous un angle procédural, Serge GUINCHARD, « Une *class action* à la française ? », art. préc., spéc. p. 2185.

[1555] Geneviève VINEY, art. préc., spéc. p. 2953.

l'existence [1556]. S'agissant enfin de l'affectation des profits restitués par le « spammeur », plusieurs possibilités seraient envisageables comme nous l'avons précédemment exposé : soit opter pour une répartition à parts égales entre toutes les victimes qui se seraient manifestées à la suite de la publication de la décision, soit pour le versement de tout ou partie de l'indemnité à un fonds d'aide aux victimes de dommages de masse [1557]. Comme nous l'avons soutenu précédemment, il semble que la solution médiane, qui consiste à verser une partie de montant de l'indemnité aux victimes et une autre à un fonds, apparaisse la plus adéquate. En effet, elle permettrait non seulement de dissiper les craintes quant à un enrichissement injustifié de la victime puisque chaque victime connue recevrait une indemnisation proportionnelle à son préjudice, mais aussi de respecter la fonction de peine privée de l'action en responsabilité engagée à l'encontre du « spammeur ».

c. Le jugement de la *class action*

503. Le dénouement de l'instance. Lorsque le juge rend sa décision sur le fond, il est essentiel que le législateur lui reconnaisse l'autorité de la chose jugée, c'est-à-dire qu'elle s'impose à l'ensemble des membres du groupe qui renonce corrélativement à exercer un recours individuel sur la question qui vient d'être jugée. En cas de procédure abusive du représentant, la condamnation de ce dernier doit être prévue afin d'éviter tout risque de dérives, sans toutefois que les autres membres du groupe puissent être affectés par cette décision. Cette solution se justifie pour des raisons pratiques : d'une part, le nombre important de membres rend inenvisageable une telle action à leur encontre mais d'autre part et surtout, elle serait considérée comme injuste, spécialement dans le cas où le législateur choisirait de consacrer le mécanisme de l'*opt-out* [1558]. Outre la voie judiciaire, le différend pourrait encore se solder par une transaction [1559], solution encouragée actuellement en France, sous réserve qu'elle soit entourée de certaines garanties. En particulier, il est essentiel de désigner clairement les personnes auxquelles elle sera opposable de façon à ce que le défendeur ne soit pas, par la suite, poursuivi par une personne qu'il pensait participer à l'action au groupe [1560]. Toujours dans un souci d'éviter d'éventuels abus, la transaction ne pourrait, à l'instar du système américain, avoir force exécutoire qu'après l'examen par le

[1556] Geneviève VINEY, art. préc., *loc. cit.*
[1557] Geneviève VINEY, art. préc., *loc. cit.*
[1558] V. en ce sens, Séverine CABRILLAC, « Pour l'introduction de la class action en droit français », art. préc., spéc. n° 39, p. 17.
[1559] Art. 2044 et s. C. civil. – V. par ex. Hervé CROZE, Christian MORAL et Olivier FRADIN, « La transaction », *in Procédure civile*, Litec, coll. *Objectif Droit cours*, 2008, spéc. pp. 228-330.
[1560] Séverine CABRILLAC, « Pour l'introduction de la class action en droit français », art. préc., spéc. n° 40, p. 17.

juge du sérieux de la transaction. Ce contrôle judiciaire pourrait prendre la forme d'une procédure d'homologation [1561].

*

* * *

504. Cette étude a permis de démontrer qu'en théorie, la réunion des conditions de déclenchement de l'action en responsabilité délictuelle en matière de *spamming* ne posait pas de difficultés pratiques majeures : le *spamming* constitue incontestablement une faute délictuelle à l'origine d'un dommage qu'il convient de réparer. Toutefois, faute de jurisprudence française en la matière, l'analyse de certaines affaires américaines nous a permis d'envisager, en pratique, comment les juges américains avaient pu reconnaître la responsabilité de prévenus poursuivis pour avoir procédé à l'envoi de *spams*. À travers ces différents exemples concrets, nous avons pu ainsi apprécier de quelle façon les tribunaux français pourraient, à leur tour, juger recevable l'action en responsabilité délictuelle engagée contre un « spammeur » dans des espèces semblables. Les limites de cette action sont toutefois apparues au stade de la réparation, tout particulièrement lorsque les « spammés » ne subissent qu'un préjudice infime. Une évolution de notre droit de la responsabilité civile délictuelle est donc apparue indispensable afin de le rendre plus efficace. Nos propositions ont ainsi porté tout d'abord sur le droit substantiel en préconisant la consécration officielle de la faute lucrative afin de permettre de prendre en compte des comportements, tels que le *spamming*, qui continuent de sévir en raison notamment des bénéfices qui peuvent être retirés malgré une éventuelle sanction. L'intégration de ce type de faute dans le droit de la responsabilité délictuelle nous a ainsi conduits à rechercher une sanction efficace. À ce titre, l'introduction dans notre droit des dommages-intérêts punitifs, inspirés du système américain, est apparue comme une sanction adaptée puisqu'elle permettrait de paralyser les profits issus de cette faute et d'ôter ainsi tout l'intérêt qui motivait leurs auteurs à poursuivre leur activité. S'agissant ensuite du droit processuel, il s'agissait de proposer une nouvelle voie permettant de mettre fin à une situation inacceptable où certains, et notamment les « spammeurs », profitent d'une activité particulièrement lucrative au préjudice de milliers de personnes. Pour cela, la reconnaissance d'une action de groupe, inspirée de la *class action* existant aux États-Unis, est apparue pertinente pour ces victimes dont le dommage est trop minime pour engager, seules, une telle action.

[1561] Art. 384, al. 2 du C. procédure civile. – V. en ce sens, Séverine CABRILLAC, « Pour l'introduction de la class action en droit français », art. préc., spéc. n° 40, p. 17 (la procédure d'homologation est la « *voie qui permet à l'heure actuelle en droit français de vérifier l'opportunité d'accords considérés comme si importants et si dangereux qu'une confiance absolue ne peut être faite à la volonté des parties* »).

SECTION II. LE *SPAMMING*, GÉNÉRATEUR DE RESPONSABILITÉ CONTRACTUELLE

505. L'interdiction du *spamming* par le contrat. Pour les besoins de cette étude, rappelons que le « spammeur » a nécessairement besoin d'une connexion à l'internet et d'un compte de courrier électronique pour poursuivre ses activités. À cette fin, il doit conclure un contrat auprès d'un FAI et d'un fournisseur de messagerie électronique, qui sont généralement une seule et même entité. Cette souscription se matérialise par une acceptation en ligne des conditions d'utilisation desdits services, acceptation expresse emportant obligation pour l'internaute de respecter l'ensemble de ces dispositions. Par cette acceptation, toute personne qui envisage d'entreprendre une activité de prospection commerciale *via* ces services, doit le faire dans les limites de cette relation contractuelle, sous peine d'engager sa responsabilité contractuelle [1562]. Une clause interdisant tout recours à

[1562] Précisons ici que nous ne traiterons pas de façon approfondie la controverse doctrinale qui existe depuis quelques années autour de la responsabilité contractuelle dans la mesure où la jurisprudence ainsi qu'une importante doctrine reconnaît l'existence d'une véritable responsabilité délictuelle. Rappelons toutefois que certains auteurs contestent la pertinence du concept même de responsabilité contractuelle, la qualifiant de « *faux concept* » en ce sens que les dommages et intérêts alloués au contractant victime n'auraient pas pour fonction de réparer un dommage mais seraient, au contraire, destinés à assurer une « *exécution par équivalent* » (v. en ce sens, Philippe LE TOURNEAU (sous la dir.), *Droit de la responsabilité et des contrats*, 8e éd., Dalloz, coll. *Dalloz Action*, 2010, spéc. n° 802 et s. p. 258 et s. – Laurence LETURMY, « La responsabilité délictuelle du contractant », *RTD civ* 1998, p. 839 et s. – Philippe REMY, « La responsabilité contractuelle, histoire d'un faux concept », *RTD civ* 1997, p. 323 et s. – Éric SAVAUX, « La fin de la responsabilité contractuelle », *RTD civ.* 1999, p. 1 et s. – Denis TALLON, « L'inexécution du contrat : pour une autre présentation », *RTD civ.* 1994, p. 223et s.). – Toutefois, la jurisprudence n'a pas cédé à cette position, et considère en effet que le responsabilité contractuelle ne peut s'analyser seulement comme un mode d'exécution de l'obligation par équivalent. La condamnation à des dommages et intérêts répond aussi à l'idée d'une réparation du préjudice causé par l'inexécution, et justifie le recours à la notion de responsabilité contractuelle. À cet égard, la Cour de cassation rappelle régulièrement que les dommages et intérêts ne peuvent être alloués que s'il existe un dommage, condition classique du droit de la responsabilité, la preuve que la prestation attendue n'a pas été réalisée étant insufisante (v. en ce sens, Cass. civ. 3e, 3 déc. 2003, pourvoi n° 02-18.033 ; *Juris-Data* n° 2003-021222 ; *Bull. civ.* III, n° 221; *JCP* 2004. I. 163, chron. G. Viney ; *RTD civ.* 1994, p. 295 et s., note P. Jourdain. – Cass. com., 13 mars 2007, *inédit*, pourvoi n° 05-20.606, *LPA* 11 sept. 2007, n° 182, p. 7 et s., note M.-L. Lanthiez. – Cass. civ. 2e, 11 sept. 2008, *RDC* 2009, p. 77, obs. O. Deshayes). – La position de la jurisprudence est également appuyée par un courant doctrinal majoritaire (v. Alain BENABENT, *Droit civil : Les obligations, op. cit.*, spéc. n° 403, p. 287. – Yvaine BUFFELAN-LANORE et Virginie LARRIBAU-TERNEYRE, *Droit civil : Les obligations, op. cit.*, spéc. n° 1480 et s., pp. 494-495. – Jean CARBONNIER, *Droit civil : Les obligations, op. cit.*, spéc. p. 155. – Jacques FLOUR, Jean-Luc AUBERT, Éric SAVAUX, *Les obligations : Le rapport d'obligations*, tome 3, Sirey, coll. *Sirey Université*, 2009, spéc. n° 171 et s., p. 137 et s., et plus particulièrement sur la nécessité d'un dommage (*id.*, spéc. n° 216, p. 187). – Muriel FABRE-MAGNAN, *Droit des obligations : Contrat et engagement unilatéral*, 2e éd., P.U.F., coll. *Thémis droit*, 2010, spéc. pp. 647-648 et 679 et s. – Christian LARROUMET, *Les obligations : Le contrat, 2ème partie : Les effets*, 4e éd., Économica, 2007, spéc. n° 643, p. 712 ; « Pour la responsabilité contractuelle », *in Le droit privé français à la fin du XXe siècle, Études offertes à Pierre CATALA*¸. *op. cit.*, p. 543 et s. – MALAURIE, Laurent AYNES et Philippe STOFFEL-MUNCK, *Droit civil : Les obligations, op. cit.*, spéc. n° 997, p. 545 et s. – Patrice JOURDAIN, « Réflexion sur la notion de responsabilité contractuelle », *in Les métamorphoses de la responsabilité, 6e journée R. Savatier*, tome 32, P.U.F., coll. *Publications de la Faculté de droit et de sciences sociales de Poitiers*, 1998, p. 65 et s. – Geneviève VINEY a rappelé la distinction existant *« entre le droit à l'exécution de l'obligation contractuelle, qui est un effet direct du contrat et n'est donc nullement subordonné à la preuve d'un préjudice et le droit à la réparation du dommage contractuel, qui n'entre en jeu qu'à partir du moment où le créancier constate l'impossibilité d'obtenir l'exécution ou renonce à celle-ci mais qui suppose alors la preuve d'un dommage* » (chron. sous Cass. civ. 3e, 3 déc. 2003, arrêt préc. et 9 juill. 2003, *JCP* 2004, éd. G., I. 163) ; *Introduction à la responsabilité civile, op. cit.*, spéc. n° 166-15 et 166-16, pp. 416-417. – Geneviève VINEY et Patrice JOURDAIN, *Les conditions de la responsabilité, op. cit.*, spéc. n° 247. – Cette conception d'une véritable responsalité contractuelle est aussi soutenue par le projet CATALA (art. 1352). –

la pratique du *spamming* est généralement insérée dans ce type de contrat. Par exemple, les conditions générales d'utilisation de FREE, un acteur majeur parmi les FAI français, dispose que : « *l'Abonné s'engage à* […] *ne pas diffuser de courriers électroniques dans des conditions illicites (par exemple spamming et e.bombing)* » [1563]. Dans la même veine, le prestataire ORANGE précise que : « [le Client] *est soumis au respect des règles de conduite prévues par la Netiquette. Le Client s'engage à : ne pas pratiquer l'envoi de messages non sollicités à un ou plusieurs destinataires (" spamming ")* » [1564]. On constate à travers ces exemples que l'interdiction du *spamming* contenue dans les contrats des FAI s'opère, soit par une mention expresse, soit par un renvoi à un code de bonne conduite plus général qui bannit également cette pratique.

506. Le non-respect des obligations contractuelles issues des conditions générales. La violation des conditions générales d'utilisation d'un FAI par un abonné « spammeur » a déjà été soumise à l'examen des juges. Dans l'affaire *Microsoft Corp. et AOL France c/ monsieur K*, les contrats d'abonnement d'accès à l'internet et de messagerie électronique auxquels un utilisateur avait souscrits, précisaient que « *les services fournis* [étaient réservés] *à un usage personnel et* [les conditions] *interdis*[aient] *l'usage commercial ainsi que le spamming* ». Par une décision en date du 5 mai 2004, le tribunal de commerce de Paris avait ainsi jugé que l'abonné, en recourant à la pratique du *spamming*, avait violé ces dispositions contractuelles et qu'il « *ne* [pouvait] *prétendre ne pas être lié par ces dispositions qu'il* [avait] *nécessairement acceptées en souscrivant les contrats en ligne* » [1565].

507. Les codes de bonne conduite contractualisés. Datant de 1995, la Netiquette, encore appelée « étiquette des réseaux », qui était destinée à tous les acteurs de l'internet [1566],

v. sur ce projet, Pascal ANCEL, « Les rapports de la responsabilité contractuelle et la responsabilité extra-contractuelle : Présentation des solutions de l'avant-projet », *RDC* 2007, p. 19 et s. – Marianne FAURE-ABBAD, « La présentation de l'inexécution contractuelle dans l'avant-projet Catala », *D.* 2007, chron., p. 165 et s. – Jérôme HUET, « Observations sur la distinction entre les responsabilités contractuelle et délictuelle dans l'avant-projet de réforme du droit des obligations, *RDC* 2007, p. 31 et s.) et la proposition de loi de 2010 (proposition d'article 1386-18 du C. civil).

[1563] Art. 9.8 « Respect de la législation en vigueur », disponible sur : https://adsl.free.fr/cgv/CGV_FORFAIT_hors_opt_01012006.pdf. – Dans le même sens, l'article 7.3 des « conditions générales d'inscription aux services haut débit NEUFBOX de SFR » dispose que : « *Le Client s'engage également à ne pas utiliser le Service* […] *à des fins publicitaires ou promotionnelles ou d'envoi en masse de courriers électroniques non sollicités (par exemple "spamming" et "e.bombing"*), disponible sur : http://mkg.sfr.fr/docs/conditions/cgi_res_hd.pdf.

[1564] Art. 3 « Conditions d'utilisation de la messagerie électronique », disponible sur: http://assistance.orange.fr/telechargement/cgu/Messagerie.electronique_1.pdf.

[1565] T. com. Paris, 6e ch., 5 mai 2004, *Microsoft Corp. et AOL France c/ monsieur K.*, *Gaz. Pal.* 12 oct. 2004, n° 286, p. 36, note E. Garnier ; *Comm. com. électr.* déc. 2004, comm. 164, note P. Stoffel-Munck. – V. ég. T. com. Nanterre, 15 mars 2006, *LBVH c/ Wanadoo*, RG : 2004F01632.

[1566] La Netiquette est définie par la norme RCF 1855 diffusée en octobre 1995, disponible sur : http://www.rfc1855.net/, http://networketiquette.net/ (en anglais), la version française est disponible sur :

particuliers ou professionnels, fixait un ensemble de règles de bonne conduite que tout internaute devait respecter dans la cadre des diverses communications électroniques – forums de discussion, chats, *e-mails* ... [1567] – et qui interdisait déjà la pratique du *spamming*. En 2001, par exemple, le tribunal de grande instance de Rochefort-sur-Mer avait sanctionné le *spamming* pratiqué sur des forums de discussion sur la base de la Netiquette alors même que cette dernière n'était pas visée au contrat d'accès à l'internet, lui conférant ainsi la valeur d'usage au sens de l'article 1135 du Code civil [1568]. Par la suite, de nombreux fournisseurs dont les contrats se révélaient lacunaires quant à l'interdiction du *spamming* n'ont pas hésité à renvoyer expressément à la Netiquette dans leurs contrats d'abonnement. Ce procédé a d'ailleurs été validé par la cour d'appel de Paris en 2002 [1569], les juges ayant considéré que le contenu de la charte visée au contrat avait force de loi entre les parties au même titre que le contrat lui-même. Cette décision témoigne ainsi de la reconnaissance de la force juridique de l'approche autorégulatrice par le biais contractuel. Si aujourd'hui les contrats des prestataires sont plus étoffés, il n'en demeure pas moins que les règles déontologiques visées dans un code de bonne conduite continuent à être intégrées à ces contrats [1570] et font dès lors partie d'un même ensemble contractuel dont le non-respect entraînera des conséquences identiques.

508. La résiliation du contrat, un effet dissuasif ? Pour mener à bien ses activités, tout « spammeur » doit disposer, à titre préalable, d'un accès à l'internet et d'un

---

http://netiquette.fr/ et http://www.afa-france.com/netiquette.html. Parmi les règles fixées par la Netiquette figurent par exemple interdit notamment l'envoi de chaînes d'*e-mails*, préconise de préciser l'objet du message et que celui-ci corresponde au contenu dudit message, que l'expéditeur s'identifie. – Sur la nétiquette, v. Laure MARINO, note sous TGI Paris, ord. réf., 15 janv. 2002, *Monsieur P. V. c/ Sté Liberty Surf et Sté Free*, jugement préc., *D.* 2002, p. 1544 et s., spéc. pp. 1545-1546.

[1567] À titre d'exemple plus récent, on peut citer le guide des bonnes pratiques (« *Sender Best Communications Practices* ») publié en 2007 par le *Messaging Anti-Abuse Working Group* (MAAWG), une organisation internationale chargée de protéger les messageries électroniques, et élaboré en partenariat avec des FAI et des sociétés de prospection recourant habituellement à l'envoi massif de courriers à caractère commercial. v. MAAWG, *E-Marketers, Senders, ISPs Fight Spam with New MAAWG Sender Best Practices Endorsed by Industry*, disponible sur : www.maawg.org/news/maawg070515.

[1568] TGI Rochefort-sur-mer, 28 févr. 2001, *Monsieur Christophe G c/ SA France Telecom Interactive*, jugement préc.

[1569] En effet, dans cette espèce, la cour a relevé que « *l'abonné est considéré comme ayant accepté sans réserve les conditions générales de* [la société LIBERTY SURF] *lorsqu'il aura cliqué sur la cas "Valider"* », conditions auxquelles était annexée une charte de bonne conduite « *interdisant notamment l'envoi en nombre de messages non sollicités et d'autres faits de type "spamming"* » (CA Paris, 11 oct. 2002, n° RG : 2002/09099 confirmant TGI Paris, ord. réf., 15 janv. 2002, *Monsieur P. V. c/ Sté Liberty Surf et Sté Free*, jugement préc.).

[1570] Cette démarche est classique dans les contrats d'accès et d'utilisation des services de l'internet et s'inscrit dans la tendance actuelle à la multiplication des codes de bonne conduite auxquels les FAI français et européens se réfèrent afin de protéger les mineurs et de lutter contre les contenus illicites et notamment ceux à caractère pédo-pornographique, raciste ou antisémite ou contre la piraterie électronique (V. site de l'Association française des Fournisseurs d'Accès et de Services Internet (AFA) qui regroupe les prestataires techniques chargé de l'accès, de l'hébergement, des moteurs de recherche mais aussi des réseaux communautaires, disponible sur : http://www.afa-france.com/p_20040329.html, http://www.afa-france.com/charte_contenusodieux.html, Charte d'engagements pour le développement de l'offre légale de musique en ligne, le respect de la propriété intellectuelle et la lutte contre la piraterie numérique disponible sur : http://www.afa-france.com/charte_musique.html. L'AFA est membre fondateur de L'EUROISPA, l'Association Européenne des Associations de Fournisseurs d'Accès et de Services Internet, disponible sur : http://www.euroispa.org).

compte de messagerie électronique lui permettant de se connecter au réseau et d'envoyer des *e-mails* grâce à le ou les contrat(s) d'abonnement qu'il aura souscrit(s). En faisant jouer la clause de résiliation figurant dans ce type de contrat, le fournisseur se ménage ainsi la faculté d'anéantir toute possibilité pour le « spammeur » de poursuivre ses agissements. L'effet d'une telle clause apparaît dès lors imparable, sous réserve qu'elle n'ait pas « *pour objet ou pour effet de créer, au détriment du non-professionnel ou du consommateur, un déséquilibre significatif entre les droits et obligations des parties au contrat* » [1571]. La violation des dispositions contractuelles – conditions générales d'utilisation et/ou code de bonne conduite – aura plusieurs conséquences à la suite d'une mise en demeure préalable [1572]. D'une part, ce manquement entraînera la résiliation du contrat d'accès à l'internet et/ou aux services de messagerie électronique après une suspension préalable [1573]. D'autre part, d'un point de vue technique, l'abonné se verra privé de son accès à l'internet. C'est ainsi que dans les affaires précitées, le non-respect des termes du contrat caractérisé par le *spamming* a, dans tous les cas, abouti à la sanction la plus sévère, à savoir la résiliation [1574]. La seule rupture du contrat par un FAI pourrait toutefois se révéler insuffisante en pratique. En effet, une fois le contrat résilié, le « spammeur » ne demeurerait pas longtemps sans accès à l'internet ou sans compte de messagerie puisqu'il pourrait s'adresser à un autre prestataire. Afin de pallier cet inconvénient, la mise en place d'une liste noire de « spammeurs » notoires par les FAI à l'échelle européenne serait un complément dissuasif non négligeable en matière de lutte contre le *spamming*.

509. Appréciation critique du recours au contrat. « *Expression d'un droit négocié* » [1575], la convention constitue un instrument privilégié en raison des nombreuses qualités qu'elle présente, à savoir sa souplesse, son pragmatisme et sa faculté à régir tout type de situation. Au nombre des avantages qu'elle présente, on peut également citer sa force obligatoire ainsi que la prévisibilité des sanctions prévues en cas de violation du contrat. S'inscrivant dans une perspective d'efficacité, objectif souvent manqué par les dispositions légales, le contrat fait preuve d'une certaine flexibilité dans sa rédaction puisqu'il est capable de s'adapter au gré des évolutions des nouvelles technologies. Les dispositions contractuelles

[1571] Art. L. 132-1 C. conso.
[1572] Art. 1146 C. civil.
[1573] Par exemple, « *Le non-respect de l'une de ces stipulations entraîne la suspension puis la résiliation du service d'Accès Internet du Client* […] *et entraîne automatiquement et de plein droit la fermeture du service* ». (Art. 3 des conditions d'utilisation de la messagerie ORANGE préc.). –V. ég. art. 16.1 des conditions générales de FREE préc., article 13 des Conditions Générales d'Inscription aux Services Haut Débit NEUFBOX de SFR préc.
[1574] TGI Rochefort-sur-Mer, 28 févr. 2001, *Monsieur Christophe G c/ SA France Telecom Interactive*, jugement préc. – TGI Paris, ord. réf., 15 janv. 2002, *Monsieur P. V. c/ Sté Liberty Surf et Sté Free*, jugement préc. – T. com. Paris, 6e ch., 5 mai 2004, *Microsoft Corp. et AOL France c/ monsieur K.*, jugement préc.
[1575] Christelle BALLANDRAS ROZET, *Les techniques conventionnelles de lutte contre les pollutions et les nuisances et de prévention des risques technologiques*, Thèse, 29 novembre 2005, Université Jean Moulin – Lyon 3 – Faculté de Droit.

apparaissent dès lors plus facilement applicables pour les parties contractantes et cohérentes parce qu'elles collent précisément à la situation qu'elles ont vocation à encadrer. En effet, le contrat recèle un atout psychologique certain en ce sens que ce dernier s'inscrit dans un environnement plus proche, plus familier des parties puisque ces dernières ont nécessairement pris connaissance de l'étendue des obligations leur incombant avant de les accepter expressément. Dans ces circonstances, en raison de cette proximité, on s'attendrait à ce que les parties respectent davantage le contrat conclu qu'une loi par nature générale, et parfois moins intelligible [1576]. Malgré ses avantages, il convient de souligner que son intervention reste très limitée puisque seul le FAI contractuellement lié à un abonné « spammeur » pourra agir sur le fondement de cette responsabilité.

*

* * *

510. La technique contractuelle présente une certaine utilité au regard de la lutte anti-*spam*, rendant son essor incontournable. En particulier, la faculté de résiliation prévue dans les contrats de fourniture des FAI français apparaît radicale puisqu'elle permet d'interrompre immédiatement les services indispensables à la pratique du *spamming*. Toutefois, le contrat conclu entre un FAI et un « spammeur » potentiel soulève la question de son efficacité dans un contexte international. En effet, les FAI étrangers risquent d'adopter des politiques d'utilisation de leurs services différentes, et peut-être même plus laxistes, envers ce phénomène que celles fixées par les FAI français ou européens, en raison notamment des divergences entre les pays sur la conception du *spamming* et leur réglementation anti-*spam* [1577]. Ces contrastes mettent en évidence la nécessité d'uniformiser les clauses contractuelles entre les FAI de différents pays. Pour parvenir à cette harmonisation, il serait intéressant, par exemple, de proposer la création d'une association regroupant, à l'échelle mondiale, des acteurs du secteur des communications électroniques. Cette association serait chargée d'élaborer des contrats standards de fourniture de services que tout fournisseur pourrait mettre en œuvre et ce, quelle que soit sa nationalité [1578]. Malgré les avantages de cette proposition, il convient d'admettre que parvenir à un consensus

[1576] Jacques GHESTIN et Gilles GOUBEAUX, *Traité de droit civil : Introduction générale*, 4e éd. avec le concours de Muriel FABRE-MAGNAN, L.G.D.J., 1995, spéc. n° 552, p. 508.
[1577] Sur les difficultés qui peuvent se poser en raison des conflits entre les politiques adoptées par les différents FAI, v. not. Sabra-Anne KELIN, « State Regulation of Unsolicited Commercial E-Mail », 16 *Berkeley Tech. L.J.* 435, spéc. pp. 442–443 (2001).)
[1578] David A. GOTTARDO, « Commercialism and the Downfall of Internet Self Governance: An Application of Antitrust Law », 16 *J. Marshall J. of Comp. & Info. L.*125, spéc. pp. 141–142 (1997).

international reste utopique et même si tel était le cas, la nature collaborative d'un tel mouvement risquerait d'avoir pour effet pervers d'entraver la libre concurrence [1579].

[1579] Ce mouvement se heurterait probablement à la législation européenne et aux lois antitrust fédérales, en particulier la section 1 of the *Sherman Act* (Michael A. FISHER, « The Right to Spam? Regulating Electronic Junk Mail », 23 *Colum.- Vla J.L. & Arts* 363, spéc. p. 364 (2000)), spéc. p. 396 (citant le *Sherman Antitrust Act*, 15 *U.S.C.* Sec. 1), la législation antitrust américaine étant particulièrement rigoureuse (v. not. *Fashion Originators' Guild of Am., Inc. v. FTC*, 312 *U.S.* 457 (1941)).

CONCLUSION DU CHAPITRE 2

511. Cette étude a permis de démontrer que dans les cas les plus fréquents où le « spammeur » procède à l'envoi simultané de *spams* à une multitude de destinataires, ce dernier avait peu de chances de voir sa responsabilité engagée. En effet, dans cette hypothèse précise, le préjudice subi par chaque victime est tout à fait minime et n'incite pas les victimes à déclencher une telle action et même si elle venait à l'envisager, cette action risque d'être rejetée par les juges. Cette situation de blocage est directement liée à la nature diffuse de cette pratique : chaque « spammé » ne recevant en définitive qu'un seul *spam* lors d'une même opération de *spamming*. Dans ces circonstances, les « spammés » subissent un réel dommage, non pas en raison de ce seul *spam* mais de la réception quasi quotidienne d'importante quantités de *spams* provenant de différents « spammeurs » et qui polluent leur messagerie électronique. Afin de sortir de cette impasse, il est apparu incontournable d'envisager certains ajustements des règles gouvernant le droit de la responsabilité civile élaborées à l'origine pour une fonction réparatrice. Parmi ces aménagements, nous avons été conduits à proposer d'une part, la consécration officielle de la faute lucrative et d'autre part, celle de dommages-intérêts punitifs, à l'instar du droit américain. Si cette proposition venait à être consacrée, l'action en responsabilité civile permettrait ainsi d'enrichir l'arsenal répressif existant en s'imposant comme un instrument répressif efficace pour pallier les insuffisances de la loi pénale. Enfin, l'efficacité de l'action en responsabilité civile délictuelle commande également de permettre aux « spammés » ne subissant que des dommages infimes de regrouper leurs demandes en une demande globale, en s'inspirant de la *class action* existant en droit américain. En effet, sans l'action d'une personne unique, le représentant, aucune action n'aurait sans doute ni vu le jour ni eu de chance de succès. À l'issue de cette analyse, le droit positif français apparaît ainsi perfectible et rejoint la discussion engagée sur les évolutions nécessaires à apporter à la responsabilité civile en s'inspirant de mécanismes juridiques déjà existants hors de nos frontières. Cette démarche de droit comparé est particulièrement riche puisqu'elle aboutirait en définitive à rapprocher les différentes solutions nationales. Ce souci d'estomper ces divergences nationales est d'autant plus nécessaire en matière de *spamming* que précisément, ce sont ces oppositions entre les différents systèmes juridiques qui profitent aux « spammeurs ». S'agissant de la responsabilité civile contractuelle, si la résiliation apparaît comme une sanction radicale qui permet de mettre fin immédiatement à l'action des « spammeurs », ces derniers pourront toujours conclure un contrat avec un autre FAI et poursuivre ainsi leur activité. On mesure à ce stade les limites de cette action puisque si cette dernière sera le plus souvent engagée contre les « spammeurs » les plus virulents, ceux qui mènent une activité de *spamming*

occasionnelle, voire unique, auront certainement de grandes chances d’échapper à toutes poursuites.

512. La diversité des cas de *spamming* et des atteintes portées obligent le juriste à faire preuve de sagacité afin de rechercher le fondement juridique qui apparaîtra le plus adapté aux circonstances de l'espèce. À cet égard, nous avons vu que la dangerosité du *spamming* qui se manifeste tant au regard des méthodes d'envoi que du contenu véhiculé nécessite une sanction de l'ensemble de ces cas de *spamming*. La responsabilité pénale du « spammeur » pourra ainsi être engagée sur divers fondements. Le droit pénal vient consolider la protection des « spammés » en offrant des fondements juridiques variés en pénalisant cette pratique par le biais de la condamnation du contenu qu'il véhicule mais aussi en sanctionnant les aggravations occasionnées par la réception de *spams* sur la base des atteintes portées aux systèmes informatiques ou aux données qu'ils contiennent. Pour sa part, le recours au droit commun de la responsabilité civile, tant délictuelle que contractuelle, permet en théorie de prendre en compte l'ensemble des victimes du *spamming* et d'assurer une réparation plus complète des dommages occasionnés par ce fléau. Toutefois, la responsabilité civile délictuelle telle qu'elle existe actuellement ne permet pas d'obtenir une réparation suffisante. L'analyse de l'efficacité de l'action en responsabilité en matière de *spamming* a démontré que sa fonction devait évoluer dans certaines hypothèses vers une dimension répressive. Le *spamming* a été en effet l'occasion de démontrer qu'elle doit évoluer pour devenir une action efficace dans certains contentieux : faute lucrative, dommages-intérêts punitifs, action de groupe.

513. Quoi qu'il en soit, la dimension internationale du *spamming* demeure donc un défi pour l'application effective de l'ensemble de ces textes français. En effet, les composantes du *spamming*, à savoir la collecte des données, l'envoi et la réception des messages, tout comme les « acteurs » de cette pratique – « spammeurs » et « spammés » – sont susceptibles d'être localisés sur le territoire de divers États. Dans ces circonstances, le problème du *spamming* doit être envisagé en adoptant une approche juridique du phénomène qui transcende la conception classique de la souveraineté, circonscrite à un territoire géographique strictement limité. La question de la protection des « spammés » établis en France ne peut être efficacement traitée en ignorant cette dimension internationale. En effet, implique nécessairement plusieurs États dont les juridictions pourraient elles-mêmes se déclarer compétentes et arguer de la compétence de leur loi nationale. Plusieurs interrogations surgissent et qui ne peuvent se résoudre par le seul droit national : Comment la loi française pourrait-elle efficacement appréhender un problème par nature internationale ? Comment pourrait-elle s'imposer en cas de conflit entre plusieurs lois nationales susceptibles

d’être compétentes ? Comment cette même loi pourrait-elle par exemple empêcher un « spammeur » de procéder à l’envoi de *spams* alors même que ce dernier est établi dans un État dont la législation ne la réprime pas ?, autant de questions qui imposent l’abandon nécessaire d’une logique nationale pour se tourner vers le droit international privé (Titre II.).

TITRE SECOND : L'ABANDON NÉCESSAIRE D'UNE LOGIQUE NATIONALE : LES MÉRITES DU DROIT INTERNATIONAL PRIVÉ

514. L'intervention nécessaire du droit international privé en matière de *spamming.* Comme nous avons eu l'occasion de le démontrer, les questions relatives à la protection des données à caractère personnel sont traitées de façon très hétérogène à l'échelle mondiale tout comme celles portant sur la réglementation des envois commerciaux qui divisent toujours les systèmes juridiques nationaux [1580]. Les divergences entre les régimes français et américain sont édifiantes à cet égard et risquent d'engendrer des conflits de juridictions et de lois lorsque le litige survient dans un contexte international. Pour saisir ces difficultés, prenons pour exemple l'hypothèse d'une société établie aux États-Unis envoyant des messages commerciaux à un internaute résidant en France et ce, sans avoir recueilli son consentement préalable. Ce dernier s'estime alors être victime de *spams.* En effet, selon la loi française, loi du pays de résidence du prétendu « spammé », l'envoi commercial est considéré comme illégal dès l'instant où le consentement du destinataire n'a pas été préalablement recueilli (système de *l'opt-in*). En revanche, selon la loi américaine, pays d'établissement de la société émettrice, un tel envoi n'est pas soumis au consentement préalable du destinataire ; seule une opposition ultérieure rendrait illégale les futures expéditions de courriers (système de l'*opt-out*) [1581]. À partir d'une configuration contextuelle identique, on aboutit ainsi à des solutions totalement opposées selon la loi appliquée à l'espèce considérée : un expéditeur, considéré comme « spammeur » selon la loi française, aurait plus de chance d'échapper à toute responsabilité sous l'égide de la loi américaine. Par ailleurs, quand bien même l'internaute obtiendrait, sur son territoire, un jugement prononcé en sa faveur, rien ne lui assure que cette décision soit appliquée aux États-Unis en raison des difficultés qui peuvent se poser en matière de reconnaissance des jugements français à l'étranger [1582]. Ces raisons peuvent ainsi le dissuader d'engager des poursuites. C'est précisément pour éviter de telles conséquences impraticables, tant en matière législative que juridictionnelle, que le droit international privé est appelé à intervenir [1583].

[1580] Sur les oppositions entre les systèmes français et américain, v. *supra* : n° 290 et s. et 323 et s.
[1581] Sur la portée de ces deux systèmes d'*opt-in* et d'*opt-out*, v. *supra* :n° 284 et s.
[1582] Cette difficulté a trait à la question de l'efficacité des jugements rendus dans un pays étranger, v. *infra* : n° 588.
[1583] Une partie de la doctrine s'est déjà penchée sur la corrélation entre l'internet et le droit international privé, v. par ex. Marie-Élodie ANCEL, « Un an de droit international privé du commerce électronique », *Comm. Com. électr.* janv. 2007, n°1, p. 1 ; janv. 2008 ; janv. 2009, pp. 17-22. – Jean-Sylvestre BERGE, « Droit d'auteur, conflits de lois et réseaux numériques : rétrospective et prospective », *Rev. Crit. DIP* juill.-sept. 2000, p. 357 et s. – Georges CHATILLON (sous la dir.), *Le droit international de l'Internet, Bruylant*, Bruxelles, 2002. – Olivier

515. Champ de la recherche. Afin de déterminer dans les litiges de dimension internationale comme celui qui vient d'être cité en exemple, quelle juridiction compétente pourra saisir le « spammé » et quelle loi pourra valablement être invoquée au soutien de son action, le recours au droit international privé se révèle indispensable. Pour répondre à ces problématiques, deux catégories distinctes de « spammés » retiendront notre attention : les « spammés » résidant en France (lien territorial avec la France) et les ressortissants français résidant à l'étranger (lien personnel avec la France). Dans la première hypothèse, il est fréquent que le lieu de résidence coïncide avec le lieu de réception du message, en l'espèce la France [1584]. Deux conséquences en découlent. En matière juridictionnelle, toute juridiction ayant un lien avec le *spamming* est susceptible de connaître du litige, à savoir : celle du lieu d'émission du *spam*, celle du lieu de sa réception, celle de la nationalité du « spammé », celle du lieu de sa résidence, celle de la nationalité du « spammeur » et celle du lieu de sa

---

CACHARD, *La régulation internationale du marché électronique*, (préf. Philippe FOUCHARD), tome 365, L.G.D.J., coll. *Bibl. dr. privé*, 2002. – M. FALLON et J. MEEUSEN, « Le commerce électronique, la directive 2000/31/CE et le droit international privé », *Rev. crit. DIP* juill.-sept. 2002, p. 435 et s. – Bénédicte FAUVARQUE-COSSON, « Le droit international privé classique à l'épreuve des réseaux», *in* Georges CHATILLON (sous la dir.), *Le droit international de l'Internet*, Bruylant 2003, p. 55 et s. – Hélène GAUDEMET-TALLON, « Droit international privé de la contrefaçon : aspects actuels », *D.* 2008, dossier, p. 735 et s. – Michael A. GEIST, « Is there a There There? Towards Greater Certainty for Internet Jurisdiction », 16 *Berkeley Tech. L.J.* 1345 (2002). – Jérôme HUET, « Aspects juridiques du commerce électronique : approche internationale », *LPA* 26 sept. 1997, n° 116, p. 6 et s. ; « Le droit applicable dans les réseaux numériques », *JDI* 2002, p. 737 et s. – Tanguy VAN OVERSTRAETEN, « Le règlement des litiges : tribunal compétent, loi applicable et modes alternatifs de règlement », *in* Étienne MONTERO, Jan DHONT, Daniel FESLER et al., *Le droit des affaires en évolution : Le contrat sans papier*, Bruylant-Kluwer, Bruxelles-Antwerpen, 2003, p. 237 et s. – Michel VIVANT, « Cybermonde : Droit et de droits des réseaux », art. préc. – Katharina BOELE-WOELKI et Catherine KESSEDJIAN (sous la dir.), *Internet : Which Court Decides ? Which Law Applies ? Quel tribunal décide ? Quel droit s'applique ?*, Kluwer Law International, Law and Electronic Commerce, vol. 5, 1998. – En faveur de l'application du droit international privé à l'internet, v. par ex. Catherine KESSEDJIAN, évoquant les litiges sur les réseaux, observe que « *lorsqu'un litige survient, il y a immanquablement impact localisé géographiquement et territorialement. Ainsi, il n'existe aucune raison de principe pour que les règles de droit international privé ne puissent pas fonctionner* » (*Rapport de synthèse in* Katharina BOELE-WOELKI et Catherine KESSEDJIAN, *Internet : Which Court Decides ? Which Law Applies ?*, *ibid.*, spéc. p. 150). – Réfractaire à toute idée conduisant à construire des solutions entièrement nouvelles, Pierre SIRINELLI estime que « *des solutions purement internes seraient de portée limitée dans un univers où la réflexion doit être internationale* » ; « *une législation de circonstance prise en considération d'une réalité fuyante et mouvante apparaîtrait rapidement comme inadéquate ou dépassée à la première évolution technique » ;* « *le droit interne est souvent assez souple pour s'adapter à la nouvelle donne* » (« L'adéquation entre le village virtuel et la création normative : Remise en cause du rôle de l'État ? », Pierre SIRINELLI, « L'adéquation entre le village virtuel et la création normative – Remise en cause du rôle de l'État ? » *in Internet Which Court Decides ? Which Law Applies ? ibid*., spéc. pp. 8-9). – V. ég. Gabrielle KAUFMANN-KOHLER considérant que « *l'édification d'un système de compétence propre à Internet* […] *serait de peu d'utilité. Il est souhaitable que la compétence en matière d'Internet diverge le moins possible de la compétence régissant les situations hors réseaux* » (« Internet : Mondialisation de la communication », Gabrielle KAUFMANN-KOHLER, « Internet : Mondialisation de la communication », *in* Katharina BOELE-WOELKI et Catherine KESSEDJIAN, *Internet : Which Court Decides ? Which Law Applies ?*, *op. cit.*, p. 89 et s., spéc. p. 110). – *Contra* Matthew BURNSTEIN, « A Global Network in a Compartmentalised Legal Environment », *in* Katharina BOELE-WOELKI et Catherine KESSEDJIAN, *ibid.*, spéc. p. 27 et s. (favorable à une adaptation du droit international privé aux réalités de l'internet et notamment à l'unification d'un droit substantiel de l'internet « *unification of substantive Internet law* », soit en permettant aux tribunaux de développer une « " *Common law " of the Internet* », soit par le biais d'accords internationaux ou de traités). – V. dans le même sens, Herbert KRONKE, « Applicable Law in Torts and Contracts in Cyberspace » *in* Katharina BOELE-WOELKI et Catherine KESSEDJIAN, *ibid.*, spéc. p. 65 et s. (considérant les solutions du droit international privé comme inadéquates pour résoudre les litiges naissant sur le réseau).

[1584] Toutefois, cette hypothèse ne se vérifie pas toujours. Tel est le cas par exemple lorsque le « spammé » qui réside habituellement en France reçoit des *spams* à l'occasion d'un déplacement à l'étranger.

résidence [1585]. De la même façon en matière législative, toutes lois ayant un lien avec le *spamming* peuvent potentiellement se déclarer compétentes selon les mêmes critères de rattachement : la loi du lieu d'émission du *spam*, celle du lieu de sa réception, celle de la nationalité/résidence du « spammé » et celle de la nationalité/résidence du « spammeur ». Les questions de droit international privé soulevées par le *spamming* nous amènent ainsi à préciser, à titre préalable, les justifications qui ont conduit à recourir au droit international privé (Chapitre 1.) avant d'étudier ses applications en matière de *spamming* (Chapitre 2.).

[1585] Si les lois de nationalité et de résidence du « spammé » sont différentes des lois de nationalité et de résidence du « spammeur ».

CHAPITRE PREMIER : LES JUSTIFICATIONS DU RECOURS AU DROIT INTERNATIONAL PRIVÉ

516. Rappelons que l'objectif premier du « spammeur » est de toucher un public le plus large possible. Pour parvenir à cette fin, il a besoin de collecter sur le réseau le maximum d'adresses électroniques qui deviendront autant de futurs destinataires de *spams*. Cette opération est facilitée dans la mesure où les adresses électroniques circulent librement sans aucune frontière et peuvent dès lors être captées quel que soit le lieu de localisation des titulaires de ces données. Dans ces conditions, la collecte de données et l'envoi des messages peuvent avoir lieu en tout point du globe. L'internationalité du *spamming* présente ainsi une double nature : à la fois personnelle puisque dans la plupart des cas, la nationalité du « spammeur » et celle des « spammés » seront distinctes mais également territoriale, en raison de la dispersion géographique du *spamming* – émission et réception des messages, résidence du « spammeur » et celle du « spammé » – sur différents territoires. C'est précisément sur ces différentes hypothèses d'internationalité que porte la présente étude. Ainsi, nous nous attacherons à détailler les éléments de dimension internationale intrinsèques au *spamming* afin de mieux appréhender les répercussions au regard du droit international privé (Section I.). Nous verrons que l'absence de cadre uniforme en la matière nous conduira naturellement à orienter nos travaux vers la recherche d'une réponse juridique globale (Section II.).

SECTION I. UN FLÉAU SANS FRONTIÈRES : L'INTERNATIONALITÉ DU *SPAMMING*

517. Après avoir qualifié le *spamming* de délit plurilocalisé (§ 1.), nous nous attacherons à démontrer que cette qualification, commune à l'ensemble des délits commis sur l'internet, ne permet toutefois pas d'assimiler cette pratique aux cyber-délits auxquels la jurisprudence et la doctrine ont déjà eu l'occasion de s'intéresser. En effet, les spécificités du *spamming* justifient tout l'intérêt de lui consacrer une étude particulière (§ 2.).

§ 1. LE *SPAMMING*, UN DÉLIT PLURILOCALISÉ

518. L'ampleur des délits plurilocalisés. À l'origine, les éléments constitutifs des délit – fait générateur et dommage – étaient le plus souvent concentrés sur le territoire d'un État unique. Désormais, les situations dans lesquelles ces éléments sont dispersés sur plusieurs territoires tendent à se multiplier jusqu'à inverser la tendance initiale. Dans le monde réel, l'accroissement de ce type de délit, dit « complexe » selon la terminologie utilisée en droit international privé [1586], est patent. Il en est ainsi, par exemple, d'actes de contrefaçon ou de concurrence déloyale créant un préjudice à l'étranger, de délits de presse internationaux ou encore du déversement de déchets sur l'espace maritime ou terrestre d'un pays et produisant une pollution dans les eaux ou sur le territoire d'un État tiers. Ce constat se confirme avec d'autant plus de force que l'utilisation croissante de l'internet n'a cessé d'accentuer cette progression (instantanéité, dématérialisation, baisse des coûts…) [1587]. Cette multiplication des délits internationaux conduit à un constat : « *aujourd'hui contrairement à hier, leur "plurilocalisation" est la règle, la localisation unique de leurs éléments constitutifs l'exception* » [1588]. Concernant plus particulièrement les comportements sur l'internet, il en résulte que dès l'instant où les agissements commis en ligne constituent un délit, leurs

[1586] L'ensemble de ces hypothèses d'éclatement des éléments constitutifs du délit sont désignés par la doctrine sous le vocable de « faits complexes ». –V. ég. Hélène GAUDEMET-TALLON qui parle de « *délits complexes* » pour désigner « *les délits dans lesquels il y a dissociation entre le lieu où se produit le fait générateur et celui où le dommage est subi* » (*Le pluralisme en droit international privé : Richesses et faiblesses (Le funambule de l'arc-en-ciel)*, *RCADI* 2005, tome 312, spéc. n° 211, p. 220).

[1587] Sur cette multiplication des délits complexes, v. Hélène GAUDEMET-TALLON, *Le pluralisme en droit international privé : Richesses et* faiblesses, recueil préc., spéc. n° 211 et s., p. 220 et s. – L'internet est en effet devenu le support de multiples délits. D'une part, il a permis le développement de délits dits « classiques », parce que déjà connus dans le monde du réel et désormais commis en ligne. Tels sont les cas par exemple, de la diffamation, de la publicité mensongère, des actes de contrefaçon ou de concurrence déloyale. D'autre part, sont apparus de nouveaux délits nés de l'avènement de l'internet, comme le *spamming.* En effet, avant que cette pratique ne se répande sur la toile, l'inondation de nos boîtes aux lettres, certes gênante, n'était pas un fait dommageable susceptible de poursuites.

[1588] Gwendoline LARDEUX, *Sources extra-contractuelles des obligations – Détermination de la loi applicable*, *J.-Cl. Droit international*, Fasc. 553-1, 2008, spéc. n° 2.

répercussions dépassent, par définition, les frontières géographiques d'un État [1589]. Tel est le cas, par exemple, d'une image ou d'un contenu diffusé sur un site *Web* et consultable par tout internaute connecté au réseau quel que soit le lieu où il se situe [1590]. L'éclatement géographique de ces cyber-délits engendre ainsi une dispersion de leurs points d'impact justifiant pleinement l'analyse de cette situation.

519. Le *spamming*, un exemple de délit plurilocalisé. Comme nous l'avons rappelé en introduction de cette étude, l'objectif des « spammeurs » consiste à toucher un public le plus large possible, indépendamment du lieu où se situent les destinataires. Dans la grande majorité des cas, il apparaît alors que le « spammeur » sera localisé dans un État et enverra des *spams* vers des destinataires établis dans divers autres pays. Dans ces circonstances, la dispersion géographique de chacun des éléments constitutifs du *spamming* – émission et réception du message – fait entrer cette pratique dans la catégorie des délits complexes plurilocalisés. Cette situation est d'autant plus facilitée que les adresses électroniques dont la collecte est indispensable au *spamming* [1591], circulent dans un espace de dimension mondiale et sont dès lors susceptibles d'être captées en tout point du globe [1592].

§ 2. LES SPÉCIFICITÉS DU *SPAMMING*

520. Un mécanisme singulier. À ce jour, l'impact de l'internet sur les diffusions de contenus litigieux a généré des contentieux internationaux sur divers fondements – atteinte aux droits de la personnalité, diffamation, atteintes aux droits de propriété intellectuelle, … – qui ont attiré l'attention particulière de la jurisprudence et de la doctrine tant françaises [1593] qu'étrangères [1594]. En revanche, le *spamming* n'a suscité que peu de

[1589] Gwendoline LARDEUX observe à cet égard que : « [l]*es cas de scission et d'éparpillement ont atteint, par l'usage d'Internet notamment, des proportions inégalées jusque-là – les sites web étant accessibles du monde entier, l'hypothèse est intrinsèquement internationale – et touchent de nombreux types de délits : diffamation, concurrence déloyale, atteinte aux droits de propriété intellectuelle, aux droits de la personnalité ...* » (*Sources extra-contractuelles des obligations – Détermination de la loi applicable*, fasc. préc., spéc. n° 57).

[1590] Sur le cas précis des atteintes aux données à caractère personnel, Laure MARINO souligne que les nouvelles technologies ont démultiplié ces risques, provoquant des conséquences inédites en raison de l'ampleur qui les caractérise : « *partant de l'idée d'épier son voisin, on en arrive à connaître presque tout de lui. C'est dans ce tout, qui marque une différence d'échelle, que les nouvelles technologies sont substantiellement différentes* » (« Les nouveaux territoires des droits de la personnalité », *Gaz. Pal.* 19 mai 2007, n° 139, p. 22 et s.).

[1591] Sur ce point, v. *supra* : n° 58 et s. et 83 et s.

[1592] Karim BENYEKHLEF constate que « *l'information n'a plus de port d'attache parce qu'elle circule librement et qu'aucune autorité nationale ne peut à elle seule contrôler ou, à tout le moins, policer les échanges d'informations* » (« Les normes internationales de protection des données personnelles et l'autoroute de l'information », *in Le respect de la vie privée dans l'entreprise*, Thémis, 1996, Montréal, p. 66 et s., spéc. p.68).

[1593] Pour un ouvrage général, v. par ex. Arnaud NUYTS (sous la dir.), *International Litigation in Intellectual Property and Information Technology*, Kluwer Law International, 2008. – V. ég. François DESSEMONTET, « Internet, la propriété intellectuelle et le droit international privé » *in* Katharina BOELE-WOELKI et Catherine

commentaires malgré son caractère intrinsèquement international. Pour autant, cette situation ne saurait se justifier en raison d'une certaine analogie entre cette pratique et les cyber-délits susmentionnés. Pour s'en convaincre, la comparaison entre le *spamming* et la diffusion en ligne d'un article diffamatoire est très instructive. Lorsqu'un article est publié sur un site *Web*, son contenu est généralement accessible à toute personne connectée au réseau, sans détermination préalable des lecteurs potentiels. Dans cette hypothèse, l'article est envoyé à un endroit fixe (le serveur) et ne pourra être consulté que par les internautes se connectant audit site. L'accès à l'information est donc subordonné à un comportement actif de la part de tout intéressé qui souhaite en connaître la teneur. Pour sa part, le *spamming* consiste à envoyer des *e-mails* à des destinataires individuellement identifiables grâce à leur adresse électronique. Avant l'expédition de ces messages, le « spammeur », à l'instar de l'auteur de propos diffamatoires, dispose potentiellement d'un champ territorial d'émission de périmètre mondial. Toutefois, le *spamming* se distingue de l'hypothèse précédente au stade de l'émission proprement dite. En effet, lors de l'envoi, le « spammeur » choisit de déployer son activité vers seulement certains destinataires dont les adresses ont été collectées. Par ailleurs, l'autre spécificité du *spamming* concerne les destinataires. En effet, contrairement aux destinataires d'une publication diffamatoire, les « spammés » subissent involontairement les envois intempestifs. Ce n'est qu'à partir de l'instant où ils ouvriront le message pour prendre connaissance de son contenu qu'ils adopteront un comportement actif. Ces particularités engendrent des conséquences spécifiques qui se manifestent tant au regard de l'impact du *spamming* que des questions de compétence.

521. La spécificité du *spamming* en termes d'impact. Reprenons la comparaison précédente entre un article diffamatoire mis en ligne et le *spamming*. Dans le premier cas, la victime unique subit un préjudice diffus, à hauteur des multiples consultations effectuées par les internautes localisés potentiellement dans n'importe quel État. En revanche, en matière de *spamming*¸ la situation est inverse : les victimes sont multiples mais les envois litigieux causent un dommage unique à chaque destinataire du *spam* considéré individuellement ; chaque envoi étant considéré comme un délit autonome. Seront ainsi dénombrés autant de

KESSEDJIAN, *Internet : Which Court Decides ? Which Law Applies ?*, *op. cit.*, p. 47 et s., spéc. pp. 24-25. – Jean-Sylvestre BERGE, « Droit d'auteur, conflits de lois et réseaux numériques : rétrospective et prospective », chron. préc. – Pierre VERON, « Trente ans d'application de la Convention de Bruxelles à l'action en contrefaçon de brevet d'invention », *JDI* 2001, p. 805 et s. ; « Innovations apportées dans le contentieux de la propriété industrielle par le règlement 44/2001 du 22 décembre 2000 », *RDPI* mars 2001, n° 121, p. 4 et s. – Marie-Élodie ANCEL, « La contrefaçon de marque sur un site Web : Quelle compétence intracommunautaire par les tribunaux français ? », *in Droit et technique – Études à la mémoire du professeur Xavier Linant de Bellefonds*, *op. cit.*, p. 1 et s.

[1594] Pour des exemples d'actions délictuelles en droit américain, v. Gabrielle KAUFMANN-KOHLER, « Internet et mondialisation de la communication », *in* Katharina BOELE-WOELKI et Catherine KESSEDJIAN, *Internet : Which Court Decides ? Which Law Applies ?*, *op. cit.*, spéc. pp.104-108. – V. ég. Matthew BURNSTEIN, « A Global Network in a Compartmentalised Legal Environment », art. préc., spéc. pp. 24-25.

délits qu'il y a de messages expédiés ; chaque activité délictuelle s'accomplissant et produisant des effets sur des destinataires distincts qui peuvent être localisés sur des différents territoires [1595]. Ces deux hypothèses se distinguent ainsi non seulement du point de vue du nombre de victimes mais aussi de l'ampleur du préjudice éprouvé par chacune d'elle, les conséquences étant diffuses pour l'une (diffamation), concentrées pour l'autre (*spamming*).

522. La spécificité du *spamming* sur les questions de compétence. La victime de propos diffamatoires qui souhaite engager une action en justice, pourra potentiellement poursuivre le défendeur devant les juridictions de chaque État où le message est susceptible d'être lu, cette situation pouvant entrainer une multitude de lois et de juridictions compétentes. À l'inverse, en matière de *spamming*, le choix offert à la victime sera plus réduit puisque seules les lois et juridictions ayant un lien avec le *spamming* en cause auront vocation à être compétentes. À ce stade, la question reste de savoir quelle juridiction le « spammé » pourrait saisir et quelle loi s'appliquerait. Les alternatives pourront s'orienter soit en considération de facteurs géographiques – le lieu d'émission du message ou celui de sa réception – soit de facteurs personnels – nationalité ou résidence du « spammeur » ou de celle du « spammé ».

*****

*** * ***

523. Si la dimension internationale du *spamming* n'a pas suscité pour le moment un réel débat faute de contentieux avant tout, il convient toutefois de souligner que les divergences entre les systèmes juridiques quant à la protection des données à caractère personnel et aux envois commerciaux risquent de soulever de sérieuses difficultés en pratique que nous identifierons par la suite. En effet, la dispersion géographique des éléments constitutifs du *spamming* suscite questionnement dès lors que plusieurs victimes de *spams* souhaitent engager une action en justice contre un « spammeur » unique.

[1595] v. Pierre BOUREL, *Les conflits de lois en matière d'obligations extra-contractuelles*, (sous la dir. d'Henry SOLUS), (préf. Yvon LOUSSOUARN), tome XXII, L.G.D.J., coll. *Bibl. dr. privé*, 1961, p. 65 (« *il y a " parcelles d'activités extracontractuelles lorsque les faits s'irradient sur les territoires de plusieurs pays et peuvent dès lors être constitutifs de délits ou de quasi-contrats entièrement distincts* ». En conséquence, cette « *pluralité d'activités extracontractuelles entraîne sur le terrain de la solution du conflit de lois, une pluralité de rattachements des obligations extracontractuelles* » (*id.*, spéc. p. 69)). – En matière de contrefaçon, les tribunaux ont considéré les faits comme des délits différents (v. Gwendoline LARDEUX, f *Sources extra-contractuelles des obligations – Détermination de la loi applicable*, fasc. préc., spéc. n° 55).

SECTION II. À LA RECHERCHE D'UNE RÉPONSE JURIDIQUE GLOBALE

524. En raison de l'ampleur internationale du *spamming* qui mine la confiance des internautes, réduit la productivité des entreprises et freine l'activité des FAI, les instances internationales ont pris conscience de l'importance d'apporter une réponse globale par le biais d'une coopération de plus en plus étroite entre les États. Les diverses initiatives internationales menées contribuent activement à la lutte contre le *spamming*, et justifient donc leur présence au sein de cette étude. Toutefois, en l'absence de caractère contraignant et d'adhésion à l'échelle mondiale, leur participation ne peut suffire à apporter à elles seules une solution efficace destinée à régler le problème dans son ensemble (§ 1.). Dans ce dessein, s'imposerait une réglementation uniforme qui hélas n'a toujours pas été adoptée. Aussi, cette absence conduit nécessairement à se tourner vers les mécanismes offerts part le droit international privé (§ 2.).

§ 1. LES INSTANCES INTERNATIONALES : UNE ACTION INSUFFISANTE

525. Le rôle de l'OCDE. En matière de *spamming*, l'Organisation de Coopération et de Développement Économique (OCDE) [1596] a appelé à une coordination active et étroite des États. À cette fin, elle a mis en place un groupe de travail destiné à réfléchir sur les diverses actions à entreprendre pour mener une lutte efficace contre le *spamming*. L'une des premières interventions de ce groupe en 2006 a abouti à la mise en place d'une « Boîte à outils anti-*spam* » (« *Toolkit Antispam* ») [1597]. Ce document a pour but de proposer une politique de lutte anti-*spam* uniforme parmi des États membres de l'OCDE, notamment par le biais d'une coopération transfrontalière renforcée et d'une meilleure collaboration entre les outils techniques, réglementaires et répressifs, tout en veillant à leur application au niveau national mais aussi international. Elle a en particulier adopté en avril 2006, dans le cadre de cette « Boîte à outils anti-*spam* », des recommandations relatives à la coopération transfrontière dans l'application des législations anti-*spam*, encourageant ainsi les autorités chargées de faire appliquer la loi à l'échange d'informations et à la collaboration. On ne peut que déplorer que ces recommandations restent un vœu pieux dans la mesure où elles n'ont été suivies d'aucune réglementation globale.

[1596] Disponible sur : http://www.oecd.org
[1597] Pour plus d'informations sur cette initiative, v. les adresses suivantes : http://www.oecd.org/document/62/0,2340,fr_2649_201185_36488717_1_1_1_1,00.html et http://www.oecd-antispam.org/, http://www.oecd.org/document/26/0,3746,fr_2649_22555297_34888154_1_1_1_1,00.html.

526. Des initiatives européennes. La Commission européenne, consciente de la dimension internationale du phénomène, a fait de la lutte anti-*spam* une de ses priorités dans le secteur des NTIC. Elle a, à ce titre, entrepris plusieurs projets en étroite collaboration avec les États membres [1598]. Le champ de ses initiatives est particulièrement large puisque la Commission agit à la fois dans un cadre multilatéral, à travers les discussions entreprises avec l'OCDE [1599] et l'Union Internationale des Télécommunications (UIT) [1600], mais aussi bilatéral, notamment avec la FTC et l'*Asia-Europe Meeting* (ASEM) [1601]. Enfin, elle a également mis en place plusieurs programmes parmi lesquels on peut citer le *Safer Internet Plus* qui, sans avoir force obligatoire, est destiné à encourager une utilisation plus sûre de l'internet et des nouvelles technologies [1602]. Par ailleurs, plusieurs organismes ont été créés à son initiative. Tel est le cas notamment du *Contact Network of Spam Authorities* (CNSA), un réseau d'autorités nationales anti-*spam* qui se réunit régulièrement, échange sur les meilleures pratiques et coopère en matière d'application de leurs lois nationales [1603]. Son

[1598] Son champ d'action est relativement large puisqu'il s'agit d'utiliser tous les moyens existants pour servir cette cause. Elle a recours à des instruments tant législatifs, judiciaires que techniques et insiste également sur l'importance d'une meilleure sensibilisation et éducation des acteurs de l'internet.

[1599] Les 2 et 3 février 2004, la Commission européenne a accueilli un atelier anti-*spam* afin de permettre aux États membres de L'OCDE une meilleure compréhension du *spamming* et ce, afin d'aboutir à une lutte coordonnée. Il s'agissait pour les participants de recenser notamment les caractéristiques du *spamming*, ses sources, d'examiner les différentes stratégies de lutte et d'en déduire leur degré d'efficacité afin d'intensifier la coopération internationale (pour un panorama des actions de la Commission européenne en 2005, v. l'adresse suivante : http://www.ddm.gouv.fr/IMG/pdf/captef_eu.pdf).

[1600] L'UIT a notamment créé une base de données qui répertorie l'ensemble des législations anti-*spams* existantes à l'échelle mondiale, (pour un panorama des activités de l'UIT dans la lutte contre le *spamming* en 2006, consulter l'adresse suivante : http://www.ddm.gouv.fr/IMG/pdf/uit_270306.pdf).

[1601] Une conférence Asie-Europe ayant pour objectif de mener une campagne de lutte commune contre les *spams* en provenance d'Europe et d'Asie. Dans une déclaration commune adoptée lors de la conférence tenue les 21 et 22 février 2005, les pays européens et treize pays asiatiques – Brunei, Birmanie, Cambodge, Chine, Indonésie, Japon, Corée, Laos, Malaisie, Philippines, Singapour, Thaïlande, et Vietnam – ont encouragé les États à élaborer des stratégies de lutte à l'échelle nationale. Cette déclaration appelle en particulier les gouvernements à adopter des législations nationales adaptées à la lutte contre le *spamming* et les entreprises à mettre en place des stratégies de lutte anti-*spam*, tout en intensifiant la coopération internationale.

[1602] Décision n° 854/2005/CE du Parlement européen et du Conseil du 11 mai 2005 instituant un programme communautaire pluriannuel visant à promouvoir une utilisation plus sûre de l'internet et des nouvelles technologies, J.O.U.E. n° L 149 du 11 juin 2005, p. 1 et s. –. Succédant au plan d'action *Safer Internet* (1999-2004), le nouveau programme qui s'étalait sur les années 2005 à 2008 visait à explicitement à combattre le *spamming* (pour de plus amples informations, consultée l'adresse suivante : http://europa.eu/legislation_summaries/information_society/l24190b_fr.htm et http://www.telecom.gouv.fr/rubriques-menu/soutien-financements/programmes-aides/europe/safer-internet-plus/72.html. – Pour un bilan du programme *Safer Internet Plus* , v. Communication de la Commission au Parlement européen, au Conseil, Comité économique et social européen et au Comité des régions, Évaluation finale de la mise en œuvre du programme communautaire pluriannuel visant à promouvoir une utilisation plus sûre de l'internet et des nouvelles technologies en ligne, 18 févr. 2009, COM/2009/0064/final, disponible sur : http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52009DC0064:FR:NOT (le bilan est positif, les objectifs sont atteints car le programme a su s'adapter aux besoins afin de renforcer la sécurité sur l'internet. Le rapport d'évaluation préconise d'accentuer les efforts pour l'avenir sur différents points, notamment : la soutien actif au programme par tous les acteurs au niveau national, la coopération avec les pays tiers, une stratégie de communication plus active, l'amélioration de la visibilité des lignes d'urgence (*hotline*), une plus forte participation des entreprises du secteur, …).

[1603] La France est particulièrement active dans l'ensemble des enceintes internationales et européennes (OCDE, UIT…) et est, en autre, le pays leader de la « *taskforce* » de l'OCDE contre le *spamming*. Elle a été chargée pendant un an de la direction du programme CNSA (v. Direction du développement des médias, « *Les politiques publiques françaises de lutte contre le spam* », mars 2005, disponible sur : http://www.ddm.gouv.fr/IMG/pdf/captef_franceddm-3.pdf).

travail consiste à définir une procédure commune destinée à faciliter le traitement des plaintes transfrontalières relatives au *spamming* grâce à un partage plus intensif des informations. À ses côtés, a été mise en place en 2004 [1604] l'Agence Européenne chargée de la sécurité des réseaux et de l'information (l'*European Network and Information Security Agency* (ENISA)) qui travaille en étroite collaboration avec les institutions de l'Union européenne et les États membres afin d'améliorer la sécurité des réseaux informatiques. À cet égard, l'ENISA a notamment publié en décembre 2009 un rapport analysant les mesures mises en place par les FAI européens pour réduire le volume de *spams* reçus dans les messageries électroniques [1605]. Ici encore, le maître mot reste la coopération mais sans qu'aucune réglementation internationale n'ait pu émerger.

527. La collaboration des secteurs privé et public. Au soutien des actions de ces instances internationales ou européennes, on compte un certain nombre d'initiatives réunissant à la fois les secteurs public et privé. Cette forme de collaboration peut s'initier par un simple dialogue entre les acteurs de ces deux mondes. On peut apprécier, à ce titre, l'action de la *StopSpamAlliance* [1606] qui, regroupant en son sein des institutions publiques internationales et régionales en matière de télécommunications, se veut être un véritable lieu de rencontres et de dialogues afin de renforcer la lutte anti-*spam* à l'échelle internationale. Ce type de partenariat peut également se concrétiser sous la forme d'un rassemblement de ces deux secteurs au sein d'une seule et même structure destinée à rechercher une solution où seraient prises en compte la technique, la réglementation et le marché. Le *London Action Plan* (LAP) [1607] en est l'une des illustrations les plus abouties [1608]. On peut citer à ce titre

[1604] Règl. (CE) n° 460/2004 du Parlement européen et du Conseil du 10 mars 2004 instituant l'Agence européenne chargée de la sécurité des réseaux et de l'information, J.O.U.E. n° L 77 du13 mars 2004, p. 1 et s.

[1605] Le rapport est accessible à l'adresse suivante : http://www.enisa.europa.eu/act/res/other-areas/anti-spam-measures. – L'ENISA a publié deux rapports, l'un intitulé " Botnets : Measurement, Detection, Disinfection and Defence " qui établit une liste de recommandations à l'intention des adminsitrations, oragnisations gouvernementales, entreprises et particuliers pour lutter contre les *botnets* (7 mars 2011, disponible sur : http://www.enisa.europa.eu/act/res/botnets/botnets-measurement-detection-disinfection-and-defence), l'autre intitulé : " *Botnets : 10 Though Questions* " qui posent les défis que les États ont à relever pour lutter efficacement contre les *botnets* (7 mars 2011, disponible sur : http://www.enisa.europa.eu/act/res/botnets/botnets-10-tough-questions).

[1606] Consulter le site disponible sur : http://stopspamalliance.org/. – La *StopSpamAlliance*, littéralement l'Alliance pour arrêter le *spam*, est une organisation internationale issue de l'initiative internationale conjointe d'*Asia-Pacific Economic Commission* (APEC), le CNSA de l'UE, l'*International Telecommunication Union* (UIT), le Plan d'actions de Londres (LAP), l'OCDE et le *Seoul-Melbourne Multilateral Memorandum of Understanding* (Mémorandum d'entente Séoul-Melbourne) (MoU) (v. *infra*). Quatre partenaires associés l'ont rejoint en 2007 : la Télécommunauté Asie-Pacifique (APT), le Groupe de travail contre les abus de la messagerie (MAAWG), l'Internet Society (ISOC) et la Coalition Asie-Pacifique contre le courrier électronique commercial non sollicité (APCAUCE).

[1607] Pour une présentation de ce plan et le calendrier des évènements, v. le site disponible sur : http://www.londonactionplan.com. – Les membres de ce plan comptent une soixantaine d'agences de protection de la vie privée, de protection des consommateurs ou de réglementation des télécommunications d'une trentaine de pays.

[1608] Le LAP regroupe en son sein des constructeurs informatiques, des fournisseurs de services en ligne et des agences nationales de protection de données personnelles qui ont adopté un plan de lutte anti-*spam* commun.

deux de ses actions les plus notables : d'une part, l'*Operation Secure Your Server*, à visée éducative [1609] ; d'autre part, l'*Operation Zombies*, destinée notamment à préconiser des mesures permettant d'éviter que les parcs informatiques ne deviennent un réseau de PC zombies [1610]. Parallèlement à ce tandem classique entreprises/entités publiques, on dénombre des programmes à l'initiative d'organisations non gouvernementales (ONG), tels que le *Spamhaus Project* qui se place dans une logique pratique de coopération, ce dernier mettant à disposition des FAI, des grandes entreprises, des universités, des réseaux militaires et gouvernementaux, une base de données regroupant les adresses IP des « spammeurs » connus [1611].

§ 2. L'EMPRUNT NÉCESSAIRE AUX MÉCANISMES DE DROIT INTERNATIONAL PRIVÉ

528. Le recours nécessaire à la méthode des conflits de lois. Face à un phénomène de dimension internationale tel que le *spamming*, la solution la plus adaptée serait de disposer d'une norme internationale substantielle [1612] (traité international, par exemple). Cela permettrait en effet d'avoir directement accès à un droit applicable au litige considéré et d'obtenir des décisions uniformes et cohérentes. Toutefois, parvenir à doter le droit international de telles règles universelles suppose l'accord entre tous les États, ce qui s'avère en pratique très difficile à réaliser. En matière de *spamming*, les divergences entre les États compromettent fortement les chances d'atteindre cet objectif. À défaut de réglementation internationale, les situations de *spamming* qui présentent des éléments d'extranéité [1613] risquent de se voir appliquer différentes lois nationales substantielles. En l'absence de hiérarchie entre ces lois, elles se retrouveront en concurrence, une situation pouvant induire de graves inconvénients. En effet, si elles sont appliquées de façon

[1609] Cette opération a vocation à mener des campagnes de sensibilisation des grandes entreprises et des FAI à travers le monde, afin de les avertir des vulnérabilités de leur équipement informatique et des moyens de se protéger.

[1610] L'*Operation Zombies* a pour mission de communiquer les bonnes pratiques à adopter pour identifier les origines des *spams* reçus, tout en encourageant et organisant des procédures de coopération entre les différents acteurs (régulateurs et secteur de l'industrie, notamment).

[1611] À ce titre, elle met notamment à leur disposition une base de données regroupant les adresses IP de « spammeurs » connus (« *Spamhaus Block List* » (SBL)), disponible sur : http://www.spamhaus.org/sbl/), une autre répertoriant la liste des « spammeurs » identifiés comme les plus menaçants et qui ont été chassés plus de trois fois de leur FAI (*ROKSO* (*Register of Known Spam Operations*), disponible sur : http://www.spamhaus.org/rokso/).

[1612] Tel est le cas, par exemple, en matière de vente internationale de marchandises, les règles matérielles issues de la Convention de Vienne du 11 avril 1980 sont directement applicables ; toutefois tous les États ne sont pas liés par la Convention, il faut bien recourir à des règles d'applicabilité (v. par ex. Vincent HEUZE, « La vente internationale de marchandises : droit uniforme », (sous la dir. de Jacques GHESTIN), L.G.D.J., coll. *Traité des contrats*, 2000).

[1613] Jean-Luc ELHOUEISS, « L'élément d'extranéité préalable en Droit international privé », *JDI* 2003, p. 9 et s.

cumulative, cela revient à désigner la loi la plus sévère. Si on envisage une application distributive, on risque alors d'aboutir à une solution déséquilibrée où, par exemple, une même affaire se verrait appliquer telle loi nationale pour tel aspect du litige et une autre loi pour tel autre. Pour surmonter de telles difficultés, il est indispensable de se tourner vers le droit international privé qui offre une méthode des conflits de lois visant à « *pose*[r] *un critère de choix qui permette au juge de retenir une législation, et une seule, parmi les législations en présence* » [1614].

529. Le défaut de juridiction internationale. En matière juridictionnelle, le constat est identique : il n'existe à l'échelle supranationale aucune juridiction destinée à trancher les litiges internationaux qui peuvent survenir entre personnes de droit privé [1615]. Ainsi, toute situation présentant des rattachements avec plusieurs États est susceptible d'être soumise aux juges nationaux de chacun de ces États. De nouveau, une concurrence peut s'établir et justifie, dans cette hypothèse, de mettre en jeu la méthode de règle de conflit de juridictions qu'offre le droit international privé.

*

* * *

530. Le *spamming* étant par essence sans frontières, une lutte effective commanderait idéalement de parvenir à l'adoption d'une règle internationale unique, harmonieuse et impérative. L'absence de consensus sur ce point conduit naturellement à s'intéresser aux solutions proposées par le droit international privé afin d'évaluer leur pertinence en matière de *spamming.*

[1614] Pierre MAYER et Vincent HEUZE, *Droit international privé*, 10e éd., Montchrestien, coll. *Domat droit privé*, 2010, spéc. n°86, p. 68.

[1615] Il existe toutefois, dans certains domaines, des juridictions spécialisées pour connaître des litiges internationaux : en matière commerciale, on peut citer, par exemple, l'Organe de règlement des différends de l'Organisation Mondiale du Commerce (OMC) (v. le site internet de l'OMC, disponible sur : http://www.wto.org/French/tratop_f/dispu_f/dispu_f.htm) ; en matière pénale, la Cour pénale internationale (CPI) (v. son site internet disponible sur : http://www.icc-cpi.int/).

CONCLUSION DU CHAPITRE 1

531. Lorsque les éléments constitutifs du *spamming* – envoi et réception du message – ainsi que la collecte préalable des adresses électroniques sont exclusivement localisés sur le territoire d'un seul État, cette hypothèse ne soulève aucune complexité particulière pour déterminer la loi applicable et le juge compétent [1616]. En revanche, des difficultés apparaissent lorsque cette pratique présente au moins un élément d'extranéité. En effet, malgré une coopération de plus en plus étroite entre les États à l'échelle internationale, celle-ci n'a abouti ni à l'adoption d'une solution législative globale ayant force obligatoire, ni à la création d'une juridiction supranationale. Or, le caractère international que revêt si fréquemment le *spamming* est susceptible de générer une situation de conflit d'ordre juridictionnel mais aussi législatif. Afin d'éviter qu'un litige international se voit soumis à des procédures concurrentes et à des décisions contradictoires, le recours au droit international privé semble donc, en théorie, incontournable. Reste alors à examiner en pratique ses applications au cas spécifique du *spamming* afin d'évaluer la pertinence des solutions offertes.

[1616] A titre d'exemple, dans le cas où un « spammeur » français ne vise que des destinataires localisés sur le territoire français, le juge français sera compétent et la loi française aura vocation à s'appliquer sans contestation possible.

CHAPITRE SECOND : LES APPLICATIONS DU DROIT INTERNATIONAL PRIVÉ EN MATIÈRE DE *SPAMMING*

532. Contexte. Le processus du *spamming* se décompose en deux phases distinctes. La première consiste pour le « spammeur » à collecter des adresses électroniques circulant sur le réseau grâce à des logiciels aspirateurs. Une fois ces données recueillies, il pourra alors procéder aux envois à destination desdites adresses. Ces étapes – collecte et envoi – sont susceptibles d'engendrer différents types d'atteinte en fonction des victimes concernées et selon le stade auquel on se situe dans le déroulement du *spamming*. Rappelons brièvement ces divers dommages occasionnés. D'une part, les collectes d'adresses menées par les « spammeurs » portent le plus souvent atteinte à son droit à la protection des données nominatives [1617]. Dans l'hypothèse particulière où « le « spammé » est victime d'une attaque de *mail bombing,* la réception massive d'*e-mails* porte atteinte à son droit à sa tranquillité et peut engendrer la perte d'*e-mails* légitimes. D'autre part, la réception importante de *spams* peut exposer l'entreprise victime à une perturbation plus ou moins importante de son serveur de messagerie. S'agissant enfin des FAI, l'envoi massif d'*e-mails* risque d'engendrer un engorgement voire une saturation de leur réseau, les empêchant ainsi de pouvoir assurer à leurs abonnés une utilisation normale des services de courrier électronique. Il en résulte qu'à chacun des stades du processus du *spamming* (collecte et envoi), cette pratique peut engendrer une atteinte à un droit de la personnalité et/ou une faute civile délictuelle à l'origine d'un dommage.

533. Position du problème. Quelle que soit la nature de l'atteinte éprouvée, l'action en justice engagée par le « spammé » suppose alors de connaître le tribunal compétent pour trancher le litige et la loi applicable. Si aucune difficulté particulière ne se pose à l'égard de ces différents points lorsque le *spamming* est circonscrit à un territoire national, en revanche, la situation se complexifie dès lors que cette pratique s'étend au-delà des frontières d'un seul État. Cette hypothèse se vérifie dans la plupart des cas puisque, très fréquemment, « spammeur » et « spammé » sont établis dans des pays différents. L'éclatement géographique du *spamming* en divers points de contact [1618] est susceptible ainsi d'engendrer deux conséquences distinctes. D'une part, chaque État ayant un lien avec cette pratique est susceptible de déclarer ses juridictions compétentes pour connaître du litige. Plusieurs juridictions sont alors en concurrence : celle du lieu d'émission du message, celle du lieu de sa réception, celle de la résidence ou de la nationalité du « spammeur » et celle de

[1617] Sur le droit à la protection des données à caractère personnel, v. *supra :* n° 169 et s. et 180 et s.
[1618] Sur le caractère plurilocalisé du *spamming*, v. *supra* : n[os] 518-519.

la résidence ou de la nationalité du « spammé » [1619]. D'autre part, les règles internes de chaque État avec lequel le *spamming* présente un rattachement peuvent avoir vocation à régir cette même situation [1620] dans la mesure où autant de lois sont susceptibles de s'appliquer qu'il existe de rattachements possibles avec la situation de *spamming* considérée [1621] : la loi du lieu d'émission du message, celle du lieu de sa réception, celle de la résidence ou de la nationalité du « spammeur » et celle de la résidence ou de la nationalité du « spammé » [1622]. Dans ces circonstances, les questions relatives à la compétence législative et à la compétence juridictionnelle méritent d'être scrupuleusement analysées.

534. Questions à résoudre. Afin d'éviter les risques de concurrence entre plusieurs lois et/ou plusieurs juridictions nationales, il est nécessaire de désigner une juridiction unique et une loi unique parmi celles qui peuvent potentiellement prétendre être compétentes. Pour cela, l'intervention du droit international privé est destinée à résoudre ces différentes problématiques de façon ordonnée et méthodique [1623]. Dans un souci de bonne administration de la justice [1624], cette discipline permettra de désigner tout d'abord la juridiction devant laquelle le « spammé » pourra agir de façon exclusive. Cette recherche sera l'occasion de vérifier si les règles de conflit existantes en matière juridictionnelle offrent aux « spammés » résidant en France [1625] l'opportunité de saisir les juridictions françaises [1626]. Une fois que le juge s'est déclaré compétent, il devra alors désigner la loi qui a vocation à s'appliquer, l'objectif sous-jacent étant de déterminer si la loi française peut être déclarée compétente lorsque le *spamming* présente au moins un rattachement avec la France. Précisons que si les questions relatives aux règles de conflit de juridictions et de lois ne sont pas étrangères l'une de l'autre [1627], leur finalité respective doit être distinguée : tandis que les premières visent à déterminer la juridiction qui répondra le mieux aux impératifs de bonne

[1619] Sous réserve que les juridictions de la nationalité et /ou de la résidence du « spammeur » ne coïncident pas avec celles du lieu d'émission et / ou que les juridictions de la nationalité et /ou de la résidence du « spammé » ne correspondent pas à celle du lieu de réception du message.

[1620] « *Chaque loi interne* [ayant] *vocation à s'appliquer non seulement aux situations purement internes à l'État qu'il l'édicte, mais aussi bien à celles comportant un élément d'" extranéité "* » (Bernard AUDIT, *Droit international privé,* 5e éd., Economica, coll. *Corpus Droit Privé,* 2008, spéc. n° 9, pp. 7-8.)

[1621] Et plus largement de la collecte d'adresses.

[1622] Si les deux premières sont respectivement distinctes des deux dernières.

[1623] On parle ainsi de « justice conflictuelle » (sur ce point, v. Hélène GAUDEMET-TALLON, *Le pluralisme en droit international privé : Richesses et faiblesses,* recueil préc., spéc. n°s 158 -159, pp. 171-173).

[1624] C'est-à-dire pour faciliter de rassemblement des preuves, le lieu d'exécution des décisions à intervenir, privilégier la commodité des parties, pays d'exécution de la décision …

[1625] Le cas d'un Français établi à l'étranger de façon occasionnelle sera abordé dans les prochains développements, v. *infra.*

[1626] Les règles matérielles régissant la compétence internationale sont caractérisées par l'unilatéralisme : elles sont destinées à attribuer ou refuser compétence à ses tribunaux nationaux mais n'ont pas vocation à conférer compétence à des juridictions étrangères et *a fortiori* à l'écarter, chaque État étant maître des conditions dans lesquelles ses tribunaux acceptent de se saisir (sur ce point, v. par ex. Bernard AUDIT, *Droit international privé, op. cit.*, spéc. n° 12, p. 10. – Pierre MAYER et Vincent HEUZE, *Droit international privé, op. cit.*, spéc. n° 116, p. 87).

[1627] Bernard AUDIT parle de « *lien d'ordre pratique* » (*ibid.,* spéc. n° 13, p. 11).

administration de la justice et aux intérêts des parties, les secondes sont destinées à désigner objectivement la loi de l'État qui présente les liens les plus étroits avec la situation en cause [1628]. Il ne s'agit donc pas ici de résoudre la question de fond posée, en l'espèce, celle de savoir si la responsabilité du « spammeur » peut être engagée et sur quel fondement juridique. La désignation de la loi est en effet indépendante de toute considération tenant au contenu du droit désigné par la règle de conflit et au résultat auquel aboutit la réponse juridique offerte par ce droit : c'est l'expression du caractère « neutre » de la règle de conflit [1629].

535. Avant de mettre en œuvre les différentes règles de conflit applicables, il convient de répondre au préalable à la question de la qualification du *spamming* (Section préliminaire.). Une fois résolue, nous traiterons successivement la question des conflits de juridictions que génère le *spamming* (Section I.) puis celle intéressant les conflits de lois (Section II.). Cette analyse sera également l'occasion de réfléchir et d'évaluer les solutions dégagées de l'application des règles de conflit traditionnelles en matière de droit international privé afin de déterminer si celles-ci se révèlent parfaitement transposables au *spamming* ou si, le cas échéant, ses spécificités imposent certains ajustements [1630].

[1628] Sur cette distinction, v. not. Bernard AUDIT, *ib.*, n^os^ 13et 328, pp. 11 et 284-286 et Pierre MAYER et Vincent HEUZE, *Droit international privé*, *op. cit.*, spéc. n° 279 et s., p. 203 et s.

[1629] Sur ce point, v. Yvon LOUSSOUARN, « La règle de conflit est-elle une règle neutre ? », *Trav. Com. fr. DIP* 1980-1981, tome 2, p. 43 s. – Hélène GAUDEMET-TALLON, *Le pluralisme en droit international privé : Richesses et faiblesses*, recueil préc., spéc. n° 160 et s., pp. 174-193.

[1630] Nous n'évoquerons pas ici les règles de procédure, ces questions ne relevant pas des problématiques du droit international privé mais des règles étatiques de la juridiction saisie selon le principe de soumission de la procédure à la loi du for (sur ce point, v. Antoine BOLZE, « L'application de la loi étrangère par le juge français : le point de vue d'un processualiste », *D.* 2001, chron., p. 1818 et s. – Sur ce principe, v. not. Bernard AUDIT, *Droit international privé*, *op. cit.*, spéc. n^o^ 415 et s., p. 352 et s. – Pierre MAYER et Vincent HEUZE, *Droit international privé*, *op. cit.*, n° 492 et s., p. 371 et s.

SECTION PRÉLIMINAIRE. LA QUESTION DE LA QUALIFICATION EN MATIÈRE DE *SPAMMING*

536. La question de la catégorie. Avant de déterminer la juridiction compétente et la loi applicable, la méthode de la règle de conflit commande de déterminer de quelle catégorie relève la question de droit posée : obligation contractuelle ou extracontractuelle [1631]. En droit français, la distinction des obligations se fonde sur leur source, à savoir un acte juridique [1632] ou un fait juridique [1633]. L'identification de cette dernière permettra de les classer dans deux catégories distinctes de droit international privé. Les obligations de nature contractuelle naissent d'un acte juridique créé par la volonté des parties qui s'engagent mutuellement à respecter les obligations qui les lient selon des conditions (objet, durée et modalité d'exécution) qu'elles fixeront d'un commun accord. Quant aux obligations extracontractuelles, celles-ci naissent d'un fait juridique créateur d'obligations dont les contours (objet, durée et modalité d'exécution) sont fixés par la loi. De façon similaire en droit international privé, les délits relèvent de la catégorie des faits juridiques [1634].

537. Quelle qualification prêter aux relations « spammeur » et « spammé » ? Il découle du développement précédent que la nature des obligations auxquelles est tenu le « spammeur » dépend de la source dont elles découlent. À l'occasion de la collecte des adresses électroniques, le « spammeur » n'a jamais eu de contact avec la potentielle victime, cette collecte étant réalisée de façon tout à fait aléatoire. Tout lien contractuel entre le « spammeur » et le titulaire de ces données apparaît dès lors clairement inexistant. Le non-respect des obligations en matière de collecte de données fixées par la loi française relative à la protection des données à caractère personnel constitue donc un délit relevant de la catégorie des faits juridiques. S'agissant de l'envoi de *spams* proprement dit, la réponse est plus délicate et nécessite certaines précisions. Dans la plupart des cas, les dommages causés

[1631] Cette opération de qualification sera déterminante lors de la mise en œuvre du droit international privé 536 et s.). – Pour une étude approfondie sur cette opération de qualification et les problèmes qui peuvent se poser, v. Bernard AUDIT, *Droit international privé, ibid.*, spéc. n° 196 et s., p. 173 et s. – Dominique BUREAU et Horatia MUIR WATT, *Droit international privé,* tome 1, partie générale, 2e éd., P.U.F., coll. *Thémis droit*, 2010, spéc. n° 413 et s., p. 388 et s. – Pierre MAYER et Vincent HEUZE, *Droit international privé, op. cit.*, spéc. n° 148 et s., p. 119 et s. – Marie-Laure NIBOYET et Géraud DE GEOUFFRE DE LA PRADELLE, *Droit international privé,* 2e éd., L.G.D.J., coll. *Manuel,* 2009, n° 238, p. 207 et s.

[1632] « *Acte de volonté destiné (dans la pensée de son ou de ses auteurs) à produire un effet de droit* » (Gérard CORNU, *Vocabulaire juridique, op. cit.*, v. « acte juridique »).

[1633] Le fait juridique peut être défini comme tout événement quelconque auquel une règle de droit attache des effets juridiques qui n'ont pas été spécialement et directement voulus par les intéressés *(*François TERRE, Philippe SIMLER et Yves LEQUETTE, *Droit civil : Les obligations*, 10e éd., Dalloz, coll. *Précis droit privé*, 2009, spéc. n° 5).

[1634] Pierre MAYER et Vincent HEUZE, *Droit international privé, op. cit.*, spéc. n° 677 et s., p. 521 et s.

à la suite de la réception de *spams* [1635] ont pour origine des comportements susceptibles d'être poursuivis sur le fondement de la responsabilité délictuelle. Toutefois, il doit également être pris en compte le contrat conclu entre l'internaute, futur « spammeur » et son FAI. Comme nous l'avons vu précédemment, ce contrat contient très fréquemment une clause qui interdit expressément à l'abonné de recourir à la pratique du *spamming* [1636]. Tout envoi de *spams* engagera donc la responsabilité contractuelle du « spammeur » vis-à-vis de cet intermédiaire. Toutefois, cette situation se rencontre dans un contexte national où « spammeur » et FAI sont généralement établis dans le même pays [1637]. Elle ne se révèle dès lors pas pertinente dans cette étude intéressant exclusivement les cas de *spamming* ayant une dimension internationale. Cette exclusion nous conduit donc à envisager le *spamming* dans le seul cas où il relève de la matière délictuelle. Dans cette perspective, nous examinerons la question relative à la désignation de la juridiction compétente (Section I.) avant d'aborder celle concernant la loi applicable (Section II.).

[1635] C'est-à-dire l'encombrement de la messagerie électronique, le dysfonctionnement du réseau, la saturation de la bande pasante, et dans certaines hypoyhèses, l'atteinte à leur droit à la tranquillité (sur les divers dommages causés par le *spamming*, v. *supra* : n° 54 et s.).
[1636] Pour des illustrations de ces clauses, v. *supra* : n°505 et s.
[1637] L'accès à l'internet en France se fait par le biais de FAI français tels qu'ORANGE, SFR, Free, BOUYGUES TELECOM, DARTYBOX, …

SECTION I. LES CONFLITS DE JURIDICTIONS SUSCITÉS PAR LE *SPAMMING*

538. Dès lors que les victimes entendent obtenir réparation des dommages subis à la suite de la réception de *spams*, la question se pose de savoir quelle juridiction peut être saisie. En effet, le *spamming* étant par nature un délit plurilocalisé [1638], rappelons que plusieurs juridictions sont susceptibles de se déclarer compétentes pour trancher le même litige, à savoir : celle du lieu d'émission du message, celle du lieu de sa réception ou encore celle de la résidence ou de la nationalité du « spammeur » ou du « spammé ». Cette situation amène donc à déterminer si le juge français peut être déclaré compétent dès lors que la réception de *spams* ou la résidence du « spammé » est localisée en France. En l'absence de consensus ayant permis d'aboutir à une convention internationale désignant directement la compétence internationale des tribunaux français, la compétence juridictionnelle est régie par deux instruments juridiques distincts selon que le « spammeur » réside (§. 1) ou non (§. 2) sur le territoire de l'un des États membres de l'Union Européenne. Nous verrons que cette solution ne sera toutefois pas pleinement satisfaisante et nous conduira à proposer un nouveau critère de rattachement (§ 3.).

§ 1. LE « SPAMMEUR » RÉSIDANT DANS L'UNION EUROPÉENNE

539. Faute de règle de conflit de juridictions spécifique au contentieux du *spamming*, la désignation du juge compétent est gouvernée par les dispositions du règlement n° 44/2001 du 22 décembre 2000 concernant la compétence judiciaire, la reconnaissance et l'exécution des décisions en matière civile et commerciale, dit règlement « Bruxelles I » [1639], qui permet de déterminer la compétence juridictionnelle dans l'espace européen [1640]. Après avoir démontré que le *spamming* entre dans le champ d'application dudit règlement (A.), il

[1638] Sur cette qualification, v. *supra* : n° 518.

[1639] Règl. (CE) n° 44/2001 du Conseil du 22 décembre 2000 concernant la compétence judiciaire, la reconnaissance et l'exécution des décisions en matière civile et commerciale, J.O.U.E. n° L. 12 du 16 janvier 2001, p. 1 et s. – Entré en vigueur le 1er mars 2002, ce règlement s'est substitué à la Convention de Bruxelles du 27 septembre 1968 concernant la compétence judiciaire et l'exécution des décisions en matière civile et commerciale. Toutefois, la Convention de Bruxelles de 1968 continue à s'appliquer au Danemark (art. 1.3 règl. (CE) n° 44/2001 préc). – Sur cette substitution, v. not. Chantal BRUNEAU, « Les règles européennes de compétence en matière civile et commerciale : Règl. Cons. CE n° 44/2001, 22 déc. 2000 », *JCP* 2001, éd. G, I. 304. – Georges A. L. DROZ et Hélène GAUDEMET-TALLON, « La transformation de la Convention de Bruxelles du 27 septembre 1968 en règlement du Conseil concernant la compétence judiciaire, la reconnaissance et l'exécution des décisions en matière civile et commerciale, *Rev. crit. DIP oct.-déc.* 2001, p. 601 et s. – Jean-Paul BERAUDO, « Le règlement (CE) du Conseil du 22 décembre 2000 concernant la compétence judiciaire, la reconnaissance et l'exécution des décisions en matière civile et commerciale », *JDI* 2001, p. 1033 et s.

[1640] Il est à noter qu'à ce jour aucun des États membres n'a émis de réserve.

conviendra d'examiner sa mise en œuvre afin de déterminer si la juridiction française est compétente pour trancher le litige (B.).

A. LE *SPAMMING* SOUMIS A LA REGLEMENTATION COMMUNAUTAIRE

540. Conditions d'application. Le règlement Bruxelles I est applicable sous réserve du respect de trois conditions cumulatives. La première, dite temporelle, impose que toute action en justice soit intentée postérieurement à son entrée en vigueur, soit le 1er mars 2002 [1641]. La seconde, dite matérielle, posée à l'article 1.1 du règlement n° 44/2001 précise que celui-ci est applicable « *en matière civile et commerciale* » [1642], entendue comme tout ce qui relève du droit privé, à l'exclusion du droit public et du droit pénal [1643] et ce, quelle que soit la nature de la juridiction [1644]. Si ces points n'ont soulevé aucune difficulté, se posait la question de savoir si la notion de « matière civile et commerciale » devait être interprétée de manière uniforme et autonome ou devait-elle se référer au droit de l'un des États contractants. Chaque État membre ayant une conception propre des notions utilisées dans le règlement, la CJCE a souhaité éviter toute divergence quant au champ d'application du texte communautaire et s'est ainsi prononcée en faveur de la première branche de l'alternative afin de garantir l'égalité et l'uniformité des droits et obligations qui découlent du règlement pour les États membres et leurs ressortissants [1645]. Cette solution doit être saluée, d'autant plus lorsque la question de qualification concerne une notion destinée à délimiter le champ d'application du règlement. Enfin, en application de la troisième condition, dite spatiale, le règlement a vocation à s'appliquer aux litiges pour lesquels il existe un rattachement

[1641] Art. 76 règl. (CE) n° 44/2001 préc.

[1642] V. par ex. CJCE, 14 oct. 1976, *LTU c/ Eurocontrol*, aff. 29/76, *Rev. crit. DIP* 1977, p. 772, note G. Droz ; *JDI* 1977, chron., p. 707 et s., note A. Huet.

[1643] V. par ex. en ce sens Pierre BELLET, « L'élaboration d'une convention sur la reconnaissance des jugements dans le cadre du Marché Commun », *JDI* 1965, p. 833 et s., spéc. p. 850. – Berthold GOLDMAN, « Un Traité fédérateur : la Convention entre les États membre de la C.E.E. sur la reconnaissance et l'exécution des décisions en matière civile et commerciale, *RTD eur.* 1971, p. 1 et s., spéc. p. 6. – Certaines matières sont exclues de son application (art. 1.2). Il en va ainsi de l'état et de la capacité des personnes physiques, des régimes matrimoniaux, testaments et successions, des faillites, concordats et autres procédures analogues, de la sécurité sociale et de l'arbitrage. En outre, il ne recouvre pas les matières fiscales, douanières ou administratives.

[1644] Art. 1.1 règl. (CE) n° 44/2001 préc.

[1645] Comme le souligne clairement l'arrêt la Cour de justice dans *LTU c/ Eurocontrol*, arrêt préc., l'article 1.1 « *servant à indiquer le champ* [du règlement] *il importe – en vue d'assurer, dans la mesure du possible, l'égalité et l'uniformité des droits et obligations qui découlent de celle-ci pour les États contractants et les personnes intéressées – de ne pas interpréter les termes de cette disposition comme un simple renvoi au droit interne de l'un ou de l'autre des États concernés* […] *et de considérer la notion visée comme une notion autonome* » (motif 3). – Pour préciser cette notion, la Cour énonce qu'il faut l'interpréter « *en se référant, d'une part, aux objectifs et au système* [du règlement], *et d'autre part, aux principes généraux qui se dégagent de l'ensemble des systèmes de droits nationaux* ». Appliquant ces critères au cas d'espèce qui lui était soumis, elle exclut du champ d'application du règlement (à l'époque des faits, la Convention de Bruxelles) une décision rendue dans un litige opposant une autorité publique à une personne privée, où l'autorité publique a agi dans l'exercice de la puissance publique.

suffisamment étroit avec l'espace européen. Il en est ainsi notamment lorsque le défendeur est domicilié dans un État membre [1646].

541. En vérifiant l'application de ces trois conditions au *spamming*, le respect des deux premières ne donne pas lieu à discussion : d'une part, tout litige survenu après le 1er mars 2002 répond à l'exigence temporelle, d'autre part, lorsque notamment les messages ont une finalité commerciale, politique ou caritative, ils entrent alors automatiquement dans son champ d'application. S'agissant de la condition spatiale, le règlement ne sera applicable que si le « spammeur » est établi sur le territoire de l'un des États membres de l'Union européenne, indépendamment de toute considération tenant à sa nationalité [1647]. En favorisant une approche territoriale fondée sur la résidence du défendeur plutôt que celle attachée à sa nationalité, le règlement a ainsi vocation à englober le plus de situations possibles. Toutefois, le respect de cette exigence risque de réduire fortement sa sphère d'influence dans la mesure où les *spams* proviennent majoritairement de pays tiers. Dans les hypothèses où le « spammeur » réside dans l'un des États membres de l'Union européenne, le règlement Bruxelles I a vocation à s'appliquer. Sa mise en œuvre permettra ainsi de déclarer compétente la juridiction d'un des pays membres et avant tout, de déterminer si les tribunaux français peuvent être saisis du litige.

B. L'APPLICATION DU REGLEMENT EN MATIERE DE *SPAMMING*

542. Le règlement Bruxelles I attribue aux juridictions de l'État du domicile du défendeur une compétence de principe pour statuer sur une action en matière civile ou commerciale. Cette règle de compétence générale connaît toutefois de nombreuses dérogations. En particulier, lorsque l'action est de nature délictuelle, ce qui est le cas en

[1646] Art. 2.1 règl. (CE) n° 44/2001 préc. – Selon le règlement, le litige a un rattachement suffisant avec l'espace européen dans deux autres cas lorsque l'objet du litige présente certains liens de rattachement matériel avec un État membre, sans considération de domicile (art. 22). Cette disposition attribue une compétence exclusive aux juridictions de l'État membre de situation de l'immeuble pour les droits réels immobiliers et les baux d'immeubles ; celles du siège d'une société pour les questions de validité, nullité et dissolution de celle-ci ; celles du lieu de tenue d'un registre public pour les questions de validité d'inscriptions sur un registre public ; celles du lieu où le dépôt ou l'enregistrement a été demandé ou effectué pour les brevets, marques, dessins et modèles pour les litiges relatifs à leurs inscription et validité ; celles du lieu de l'exécution en matière d'exécution. Est également considéré comme un rattachement suffisant avec l'espace européen lorsque les parties ont, sous certaines conditions, attribué compétence à la juridiction d'un État membre (art. 23 et 24). En matière de *spamming*, ces deux chefs de compétence n'ont pas vocation à intervenir puisque d'une part, les matières concernées par l'article 22 ne concernent pas le *spamming* et d'autre part, l'hypothèse où « spammé » et « spammeur » auraient convenu de retenir la compétence d'un tribunal en particulier n'est pas envisageable.

[1647] Art. 2 règl. (CE) n° 44/2001 préc. – L'article 4.1 dudit règlement précise qu'à défaut, « *la compétence est, dans chaque État membre, réglée par la loi de cet État membre* ».

matière de *spamming* [1648], le demandeur peut saisir le tribunal du lieu du fait dommageable. Ces règles de compétence (1.), transposées au cas du *spamming*, révèleront que leur mise en œuvre est délicate (2.).

1. Les règles de compétence

543. Une compétence générale de principe : le for du domicile du défendeur. Selon l'article 2.1 du règlement n° 44/2001, « [s]*ous réserve des dispositions du présent règlement, les personnes domiciliées sur le territoire d'un État contractant sont attraites, quelle que soit leur nationalité devant les juridictions de cet État* » [1649]. Cette règle générale affirme donc la compétence de principe des tribunaux de l'État membre sur le territoire duquel le défendeur a son domicile [1650], ce qui correspond, pour les besoins de notre étude, à la résidence du « spammeur ». Par l'expression « [s]*ous réserve des dispositions du présent règlement* », il convient d'entendre que cette règle ne saurait souffrir d'autres exceptions que celles prévues par le règlement. Sont ainsi écartées toutes dispositions nationales, fixant des règles de compétence internationale qui auraient pour effet de faire échec à cette compétence de principe. Tel est le sort réservé par exemple aux articles 14 et 15 du Code civil français, visés à l'annexe I du règlement, qui prévoient une extension de compétence au profit des juridictions françaises, extension fondée sur le critère de la nationalité du défendeur ou du demandeur [1651].

[1648] Sur la nature délictuelle de l'action, v. *supra* : n° 537.

[1649] À noter que le texte communautaire ne vise pas un tribunal en particulier mais « les » juridictions de l'État membre, laissant ainsi la loi nationale de l'État concerné désigner le tribunal compétent (sur ce point, lire not. Bernard AUDIT, *Droit international privé, op. cit.*, spéc. n° 523, pp. 432-433). – Sur l'art. 2.1 du règlement, v. Pierre MAYER et Vincent HEUZE, *Droit international privé, op. cit.*, spéc. n° 337, p. 240.

[1650] Le règlement communautaire ne donne pas de définition communautaire de la notion de domicile et renvoie à la loi nationale du for saisi (art. 59.1 règl. (CE) n° 44/2001 préc.). Si le défendeur n'a pas de domicile dans l'État membre du for saisi, pour déterminer si elle a un domicile dans un autre État membre, le for applique alors la loi de cet État (art. 59.2). Quant aux personnes morales, leur domicile s'entend de leur siège statutaire, de leur administration centrale ou bien encore de leur principal établissement.

[1651] À l'inverse, dès lors que le « spammeur » réside dans un État tiers, le règlement Bruxelles I n'a plus vocation à s'appliquer et les règles de compétence exorbitantes des États contractants reprennent alors toute leur force. À titre d'exemple, un « spammeur », même ressortissant d'un État membre, mais domicilié en Chine, n'échappe pas au risque qu'un « spammé » domicilié en France invoque l'article 14 du Code civil pour le poursuivre devant les juridictions françaises, quelle que soit sa nationalité. En effet, l'article 2.2 du règlement Bruxelles I dispose que : « *Les personnes qui ne possèdent pas la nationalité de l'État membre dans lequel elles sont domiciliées y sont soumises aux règles de compétence applicables aux nationaux* ». Il en résulte ainsi que « *toute personne, quelle que soit sa nationalité, domiciliée sur le territoire d'un État membre, peut, comme les nationaux, y invoquer contre* » le « spammeur » l'article 14 précité (Art. 4.2 règl. (CE) n° 44/2001 préc.) et donc saisir les juridictions françaises. Cette solution est particulièrement favorable au « spammé » dans la mesure où la décision rendue bénéficie des facilités de reconnaissance dans tous les États membres, au même titre qu'un litige de dimension communautaire. Cette hypothèse témoigne du champ d'application extensif du règlement qui devient applicable dans certains cas où le litige dépasse le strict cadre européen.

544. Une compétence optionnelle : l'article 5.3 du règlement. Dans un souci de bonne administration de la justice et notamment pour faciliter l'établissement des preuves [1652], l'article 5 du règlement autorise le demandeur, et lui seul, à saisir le for d'un État membre autre que celui sur le territoire duquel est domicilié le défendeur. En particulier, aux termes de l'article 5.3 [1653], le demandeur peut agir, « e*n matière délictuelle ou quasi délictuelle, devant le tribunal du lieu où le fait dommageable s'est produit ou risque de se produire* » [1654]. La notion de « *matière délictuelle* » est considérée par la Cour de Justice des Communautés Européennes (CJCE) comme autonome [1655]. Sans en définir précisément les contours, la Cour se contente d'indiquer que cette matière « *comprend toute demande qui vise à mettre en jeu la responsabilité d'un défendeur et qui ne se rattache pas à la matière contractuelle* » [1656]. La matière délictuelle est donc définie négativement comme toute obligation qui ne découle pas d'un contrat[1657].

2. Une mise en pratique délicate

[1652] Sur ce point, v. Gabrielle KAUFMANN-KOHLER, « Internet : Mondialisation de la communication », art. préc., spéc. pp. 99-100).

[1653] Pour les besoins de notre étude, seule la dérogation fixée à l'article 5.3 du règlement relative à la matière délictuelle retiendra notre attention. Les autres dispositions de l'article 5, en raison de la nature des litiges concernés (matière contractuelle (art. 5.1) ; obligations alimentaires (art. 5.2); l'article 5.5, succursales, agences ou établissements (art. 5.5) ; *trusts* (art. 5.6) ; questions maritimes (art. 5.7)) ne couvrent pas le champ de notre étude et seront donc écartées de cette analyse. De même, ne seront pas étudiées les compétences, dites dérivées, visées aux articles 6 et 7 du règlement en cas de connexité, cette hypothèse n'entrant pas dans le champ de cette analyse.

[1654] Art. 5-3 du règl. (CE) n° 44/2001 préc. – Cette seconde option a été ajoutée lors du passage de la Convention en règlement communautaire. Toutefois, l'impact de cette évolution reste limité (en ce sens, v. Marie-Laure NIBOYET, « La révision de la Convention de Bruxelles du 27 septembre 1968 par le règlement CE du 22 décembre 2000 », *Gaz. Pal.* 10-12 juin 2001, doct., p. 943 et s. : « *Le nouvel article 5.3 n'appellerait aucun commentaire s'il n'avait pas ouvert le for du délit aux actions préventives.* […] *La solution permettra opportunément d'accueillir des actions visant à prévenir le dommage, dans les domaines où les conséquences peuvent être considréables (dommage de pollution, atteinte à la vie privée, concurrence déloyale par voie des médias, par exemple* »). – Laurent PECH, *Conflit de lois et compétence internationale des juridictions françaises, J.-Cl. Communication*, Fasc. 3000, spéc. n° 26). – Sur ces règles de compétence, v. ég. Chantal BRUNEAU, « Les règles européennes de compétence en matière civile et commerciale : Règl. Cons. CE n° 44/2001, 22 déc. 2000 », chron. préc., spéc. n^{os} 4-9 et n° 13.

[1655] Sur les difficultés entourant les notions autonomes, v. Mathias AUDIT, « L'interprétation autonome du droit international privé communautaire », *JDI* 2004, p. 789 et s., spéc. n^{os} 35 et 37, pp. 804-805 (« Lorsqu'un juge national est mis en présence d'une affaire dont il se demande si elle est soumise ou non à telle ou telle disposition d'un règlement communautaire de droit international privé, il lui appartient […] de confronter l'aspect pertinent du litige à la notion autonome résultant de la jurisprudence communautaire. Or, pour procéder à une telle opération, ses moyens sont limités. À la vérité, le seul référent dont il dispose est constitué par les termes même de la définition de la notion telle qu'elle résulte de la décision pertinente de la Cour de justice Celle-ci *n'est étayée par – pratiquement – aucun autre système de référence, en particulier textuel ou doctrinal* » (*id*., spéc. n° 37, p. 805)).

[1656] CJCE, 5^{e} ch., 27 sept. 1988, aff. 189/87, *Kalfelis*, *Rec. CJCE* 1988, p. 5565 et s. ; *Rev. crit. DIP.* janv.-mars 1989, p. 112 et s., note H. Gaudemet-Tallon ; *JDI* 1989, p. 457 et s., obs. A. Huet ; *D.* 1989, somm., p. 254 et s., note B. Audit.

[1657] Le professeur Hélène GAUDEMET-TALLON souligne toutefois à juste titre que « [d]*éfinir la matière délictuelle par opposition à la matière contractuelle qui elle-même n'a pas reçu de définition générale ne paraît pas une bonne méthode* » (note sous CJCE, 5^{e} ch., 27 sept. 1988, aff. préc., *Rev. crit. DIP* janv.-mars 1989, p. 112 et s., spéc. p. 121). – Le professeur Bernard AUDIT souligne également cette difficulté (note sous sous CJCE, 5^{e} ch., 27 sept. 1988, aff. préc., *JDI* 1989, p. 457 et s.).

545. Modalités de mise en oeuvre de l'option. L'exercice de l'option (lieu du fait générateur / lieu du dommage) appelle toutefois certaines précisions. Tout d'abord, le demandeur n'a pas à motiver sa préférence, la CJCE énonçant seulement que « *le défendeur peut être attrait, au choix du demandeur, devant le tribunal soit du lieu où le dommage est survenu, soit du lieu de l'évènement causal qui est à l'origine de ce dommage* » [1658]. Obéissant ainsi à l'idée d'une égale proximité des deux fors, justifiée par l'impossibilité de favoriser en théorie l'un des deux [1659], la victime est libre d'adopter l'une des deux branches de cette option toutes les fois où les éléments constitutifs du délit sont dissociés. Il en résulte que le demandeur peut, par exemple, choisir de saisir la juridiction du lieu du fait générateur alors même qu'il existerait des liens plus étroits avec le for du dommage. Il est évident que le choix du demandeur est motivé pour l'essentiel par la volonté de saisir les juridictions de l'État de son domicile ou à défaut, d'un État autre que celui du défendeur. Il peut également résulter de la combinaison de différents facteurs : les circonstances de l'espèce, les conditions et perspectives entourant la procédure à engager, à savoir : la facilité d'accès au tribunal, le coût et la durée du procès, les chances de succès de son action, sachant que les tribunaux sont plus enclins à appliquer leur loi nationale. En tout état de cause, ses motifs personnels ne sauraient servir d'arguments au défendeur pour contester ce choix. Cette solution est opportune car dans le cas contraire, cela aurait eu pour effet d'admettre l'exception *forum non conveniens* [1660] que la CJCE s'évertue à exclure de l'espace judiciaire européen afin de garantir la sécurité juridique.

546. Le cas des délits complexes : l'incertitude autour de la notion de dommage. Le lieu du « *fait dommageable* » auquel fait référence ce texte ne suscite aucune interrogation particulière lorsque les éléments constitutifs du délit se concentrent sur le territoire d'un même État. En revanche, la question de sa localisation reste entière en cas de dissociation du lieu du fait générateur et celui du dommage. En effet, faute de précision

[1658] CJCE 30 nov. 1976, arrêt préc., spéc. point 25.

[1659] CJCE 30 nov. 1976, arrêt préc., spéc. points 15, 17, 18, 20 et 21. – Le professeur Bernard AUDIT estime à ce titre qu' « *il n'est donc pratiquement pas possible d'éliminer l'un d'eux, chacun pouvant, selon les circonstances, se révéler spécialement approprié* » (*Droit international privé, op. cit.*, spéc. p. 443, n° 534). – Partageant ce point de vue, le professeur Gabrielle KAUFMANN-KOHLER explique qu'une solution conduisant à retenir une compétence unique n'est pas souhaitable dans la mesure où donner la priorité au lieu de l'évènement causal « *amènerait souvent une confusion avec le for du défendeur, alors que la solution inverse écarterait un for particulièrement proche de la cause du dommage* » (« Internet et mondialisation de la communication » art. préc., spéc. p. 109).

[1660] L'exception de *forum non conveniens* permet aux juridictions d'un État de refuser d'exercer leur compétence lorsqu'elles considèrent que le for saisi est inapproprié pour trancher le litige et/ou que les tribunaux d'un autre État sont mieux à même de le juger. Cette technique de droit international privé a connu un franc succès dans les droits de la *Common law* mais est étranger aux systèmes juridiques romano-germaniques. – Sur la notion de *forum non conveniens*, v. Hélène GAUDEMET-TALLON, « Les régimes relatifs au refus d'exercer la compétence juridictionnelle en matière civile et commerciale : forum non conveniens, lis pendens », *RIDC* 1994, p. 423 et s. – Pour une étude comparative de cette exception dans les pays de droit romano-germanique et ceux de la *Common law*, v. Arnaud NUYTS, *L'exception de Forum non conveniens : Étude de droit international privé comparé*, Bruylant/L.G.D.J., 2003.

apportée par l'article 5.3, aucun critère objectif ne permet de les départager. La CJCE, à l'occasion de l'affaire, dite « *Mines de Potasse* », a ainsi été conduite à expliciter la notion de « *fait dommageable* » [1661]. Elle a ainsi jugé qu'en cas de dissociation des lieux de chacun des éléments constitutifs du délit, « *l'expression " lieu du fait dommageable " doit être entendue en ce sens qu'elle vise à la fois le lieu où le dommage est survenu et le lieu de l'évènement causal* » [1662]. Cette solution, favorable au demandeur, lui permet ainsi de bénéficier d'une option de compétence juridictionnelle entre ces deux lieux [1663] et est notamment justifiée par le fait que l'un et l'autre peuvent « *selon les circonstances, fournir une indication particulièrement utile du point de vue de la preuve* [ces rattachements peuvent se révéler pertinents en raison de leur proximité avec les preuves à apporter] *et de l'organisation du procès* » [1664].

547. La question de l'étendue de la compétence de la juridiction saisie en cas de dommages multiples. Si la solution dégagée de l'arrêt *Mines de Potasse* a permis de préciser la notion de « fait dommageable » en cas de dissociation entre le lieu du fait générateur et celui du dommage, elle ne permettait toutefois pas de déterminer quel tribunal était compétent lorsqu'un même fait générateur produisait des dommages dans plusieurs pays. Telle est la question à laquelle la CJCE devait répondre, dix-neuf ans plus tard, dans l'affaire *Fiona Shevill* [1665] concernant une diffusion internationale d'articles de presse considérés comme diffamatoires par les demanderesses. La Cour a tout d'abord confirmé, dans la ligne droite de l'arrêt *Mines de Potasse*, que le lieu du fait dommageable, au sens de l'article 5.3° du règlement, devait s'entendre, soit du lieu du fait générateur, soit du lieu du dommage [1666]. Mais l'apport majeur de cet arrêt repose sur la précision introduite par la Cour quant au champ de compétence du for choisi par le demandeur. Elle a ainsi énoncé que si le for du lieu de l'événement causal, c'est-à-dire le lieu du fait générateur – en l'espèce, lieu

[1661] CJCE, 30 nov. 1976, aff. 21/76, *Sté Bier et Fondation Rheinwater c/ Sté Mines de potasse d'Alsace*, spéc. pts 24 et 25, *D.* 1977, jurispr., p. 613, note G. Droz ; *JDI* 1977, p. 728, obs. A. Huet ; *Rev. crit. DIP* 1977, p. 563, note P. Bourel. – CJCE, 11 janv. 1990, aff. C-220/88, *Sté Dumez c/ Hessische Landesbank*, spéc. pts 10 et 17, *Rec. CJCE*, I, p. 49 ; *Rev. Crit. DIP* avr.-juin 1990, p. 386 et s., note H. Gaudemet-Tallon ; *JDI* 1990, p. 497 et s., obs. A. Huet. – CJCE, 19 sept. 1995, aff. C-364/93, *Antonio Marinari c/ Lloyd's Bank et Zubaidi Trading Compagny*, spéc. pt 11, *Rec. CJCE* 1995. I. p. 2719 et s. ; *Rev. Crit. DIP* 1990, p. 368 et s., note H. Gaudemet-Tallon ; *JDI* 1996, p. 562 et s., note J.-M. Bischoff. – CJCE, 7 mars 1995, aff. C-68/93, *Fiona Shevill et al. c/ Press Alliance SA*, spéc. pt 20, *Rec. CJCE* 1995, I, p. 415, *Rev. Crit. DIP* juill.-sept. 1996, p. 487 note P. Lagarde ; *RTD eur.* 1995, p. 611 et s., note M. Gardeñes Santiago, *D.* 1996, jurispr., p. 63 et s., note G. Parléani ; *JDI* 1996, p. 543 et s., obs. A. Huet.

[1662] CJCE 30 nov. 1976, arrêt préc., spéc. point 24.

[1663] CJCE 30 nov. 1976, arrêt préc., spéc. points 19 et 25. – Cette solution rejoint l'alternative prévue à l'alinéa 3 de l'article 46 du Code de procédure civile, qui permet au demandeur de saisir « *la juridiction du lieu du fait dommageable ou celle dans le ressort de laquelle le dommage a été subi* » (Hélène GAUDEMET-TALLON, « La compétence internationale à l'épreuve du Nouveau Code de procédure civile : aménagement ou bouleversement ? », *Rev. crit. DIP* janv.-mars 1977, p. 1 et s., spéc. p. 29 et s.).

[1664] CJCE 30 nov. 1976, arrêt préc., spéc. points 11 et 17.

[1665] CJCE, 7 mars 1995, *Fiona Shevill*, arrêt préc.

[1666] CJCE, 7 mars 1995, *Fiona Shevill*, arrêt préc., spéc. pts 19, 23 et s.

d'établissement de l'éditeur de la publication litigieuse – était compétent pour connaître de l'action en réparation de l'intégralité du dommage[1667], le tribunal de chacun des lieux du dommage – lieux des diffusions de la publication diffamatoire – n'était compétent que pour statuer sur le dommage subi localement, dans son ressort territorial [1668].

548. *Quid* de l'application des arrêts de la CJCE en matière de *spamming* ? Dans les hypothèses où le « spammeur » envoie des messages à de multiples destinataires, il n'existe en réalité qu'un seul lieu du dommage pour chaque victime [1669]. On demeure donc dans une configuration de délit plurilocalisé où il existe un lieu unique du fait générateur, distinct du lieu du dommage, chaque envoi étant considéré comme indépendant. À ce stade, la solution dégagée par l'arrêt *Mines de Potasse* suffit à résoudre le conflit de juridictions envisagé. Ainsi, outre la compétence de principe du for du domicile du défendeur, le « spammé » bénéficiera de l'option lui permettant de saisir, soit le tribunal du lieu d'émission du message, lequel coïncidera le plus souvent avec celui du domicile du « spammeur », soit celui du lieu de réception, le plus souvent le for du « spammé », et ce, pour connaître de l'intégralité du dommage subi. Ce cas de figure correspond aux hypothèses les plus simples où le lieu d'émission et celui de réception de *spam* se confondent respectivement avec le lieu de résidence du « spammeur » et de celle du « spammé ». Cette transposition appelle néanmoins une série d'observations toutes les fois où le litige s'inscrit dans un cadre plus complexe.

[1667] La cour précisant que « [c]*e for coïncide toutefois, en règle générale, avec le chef de compétence de principe consacré par l'article 2, premier alinéa, de la convention* » (*id.*, spéc. pt 26).

[1668] *Id*, pt 33 (« *en cas de diffamation au moyen d'un article de presse diffusé dans plusieurs États contractants,* […] *la victime peut intenter contre l'éditeur une action en réparation soit devant les juridictions de l'État contractant du lieu d'établissement de l'éditeur de la publication diffamatoire, compétentes pour réparer l'intégralité des dommages résultant de la diffamation, soit devant les juridictions de chaque État contractant dans lequel la publication a été diffusée et où la victime prétend avoir subi une atteinte à sa réputation, compétentes pour connaître des seuls dommages causés dans l'État de la juridiction saisie* »). – La jurisprudence française avait déjà adopté cette solution, v. par ex. CA Paris, 1re ch., sect. A, 19 mars 1984, *Caroline de Monaco c/ Sté Burda Gmbh*, 1re esp., *D.* 1985, I.R., p. 179 et s., obs. B. Audit ; *Rev. crit. DIP* janv.-mars 1985, p. 141 et s., note H. Gaudemet-Tallon ; *Gaz. Pal.* 2-3 janv. 1985, nos 2-3, p. 7 et s., note J. Mauro confirmant TGI Paris, 27 avr. 1983, 2e esp., *Rev. crit. DIP* oct.-déc. 1983, p. 670 et s., note H. Gaudemet-Tallon (à propos de la diffusion en France et en Allemagne par voie de presse de photos et d'articles portant atteinte à l'image et au respect de la vie privée). – La jurisprudence a par la suite appliqué cette solution à différents cas de délits complexes, v. par ex., en matière de contrefaçon, Cass. civ. 1re 16 juill. 1997, *Époux Wegmann c/ Sté Elsevier Science Ltd*, *JCP* 1997, éd. E., pan. 1087 ; *JDI* 1998, p. 136 et s., obs. A. Huet (en l'espèce, la contrefaçon, résultant de la diffusion de publications éditées en Grande-Bretagne par la défenderesse, avait été en partie réalisée en France. La Cour de cassation, a confirmé l'arrêt de la cour d'appel aux motifs « *qu'en matière de contrefaçon, l'option de compétence posée par l'article 5.3 de la Convention de Bruxelles doit s'entendre en ce que la victime peut exercer l'action en indemnisation soit devant la juridiction de l'État du lieu d'établissement de l'auteur de la contrefaçon, compétente pour réparer l'intégralité du préjudice qui en résulte, soit devant la juridiction de l'État contractant dans lequel l'objet de la contrefaçon est diffusé, compétente pour connaître seulement des dommages subis dans cet État ; qu'en admettant sa compétence pour le seul dommage subi en France du fait de la publication réalisée en Grande-Bretagne* »).

[1669] V. *supra* (n° 44 et s.)

549. Les difficultés tenant au lieu du fait générateur. Si l'identification du lieu du fait générateur est aisée lorsque le lieu de résidence du « spammeur » se confond avec celui de l'envoi des *spams*, celle-ci devient plus délicate dans l'hypothèse où l'un et l'autre sont géographiquement dissociés. Tel est le cas notamment lorsque le « spammeur » utilise des PC zombies [1670] pour expédier ses messages. Prenons l'exemple d'un « spammeur » résidant en Allemagne qui a recours à des PC zombies situés en Espagne et destinés à envoyer des *e-mails* à des destinataires résidant en France. Le préjudice sera donc subi en France, lieu du dommage unique. Dans ce cas précis, la question se pose de savoir si le lieu du fait générateur est unique (Allemagne ou Espagne) ou multiple (Allemagne et Espagne). En effet, il convient de déterminer si le lieu du fait générateur s'entend comme celui où ont été initiés les envois, à savoir l'Allemagne, ou comme celui où est localisé l'expéditeur (malgré lui !) de l'envoi, à savoir en Espagne. En l'absence de solution dégagée par la CJCE dans le cas d'une pluralité de faits générateurs, différentes interrogations restent en suspens : la victime pourrait-elle saisir à sa convenance la juridiction de l'un ou l'autre des lieux des faits générateurs ? ou les deux ? L'incertitude qui entoure la réponse à cette question justifierait une intervention de la CJCE ou du législateur européen d'autant plus pressante que le recours à cette technique d'envoi est fréquemment utilisé par les « spammeurs ».

550. Les difficultés inhérentes à l'identification du lieu du dommage. L'identification du lieu du dommage peut également prêter à discussion au regard des évolutions technologiques. En effet, si lors des premières utilisations des services de messagerie électronique, la réception des *e-mails* avait lieu essentiellement sur des postes d'ordinateur fixes et donc, au lieu de résidence des destinataires, les progrès technologiques ont démultiplié les dispositifs facilitant la réception de courriers électroniques. Il suffit de penser en tout premier lieu aux ordinateurs portables qui ont permis aux utilisateurs de l'internet de bénéficier d'une plus grande mobilité, leur ouvrant l'accès aux services de messagerie électronique dans tout endroit où ils disposeraient d'une connexion à l'internet. Cette mobilité n'a cessé de s'accentuer au gré des avancées technologiques. On peut citer à ce titre les *smart phones* (ou « téléphones intelligents ») qui ne sont plus de simples appareils de communication vocale mais permettent également d'envoyer des courriers électroniques *via* l'internet grâce aux fonctions dont ils disposent et qui n'étaient jusqu'alors réservées qu'aux seuls ordinateurs. Ces diverses évolutions des technologies de communication offrent désormais à tout un chacun la possibilité de recevoir, de consulter ou de transmettre des *e-mails* de n'importe quel endroit du monde. Variant au gré des circonstances et des déplacements du destinataire des messages, il devient dès lors très difficile de canaliser le

[1670] Sur cette technique, v. *supra* : n° 97.

lieu du dommage et de le rattacher au lieu de réception du message, ce dernier n'apparaissant plus significatif en raison de son caractère de plus en plus fortuit.

551. La question du dommage plurilocalisé. Il est des hypothèses où le dommage peut lui-même survenir sur divers territoires. Tel est le cas, par exemple, d'un établissement principal installé en France et dont les succursales implantées en France et en Allemagne, seraient victimes de *spamming* provoquant la saturation des messageries des salariés de chacune de ces succursales [1671]. Dans ce cas de figure précis, on mesure les limites de la solution dégagée dans l'affaire *Mines de Potasse* et qui conduisent à se tourner vers celle retenue dans l'arrêt *Fiona Shevill.* Dans cette veine, on considèrerait alors que toute action destinée à obtenir réparation du préjudice subi par l'une des succursales devrait être intentée devant le tribunal du lieu d'établissement de cette dernière. En revanche, la réparation du préjudice intégral, à savoir celui subi par le groupe – établissement principal et succursales –, ne pourrait être réclamée que devant la juridiction du lieu du fait générateur, lieu d'émission des *spams*.

552. Bilan. En définitive, il apparaît que les solutions dégagées par l'application du règlement Bruxelles I au *spamming* n'offrent pas de réponses pleinement satisfaisantes au regard des incertitudes qui entourent non seulement la question du lieu du fait générateur mais aussi celle du dommage. Surtout, il ne permet pas, par définition, de traiter des cas les plus fréquents de *spamming*, c'est-à-dire lorsque le « spammeur » réside hors de l'Union européenne. Pour que notre étude soit complète, il apparaît donc incontournable de définir les règles applicables dans les cas où le règlement Bruxelles I n'a pas vocation à s'appliquer afin d'évaluer si les solutions qui s'en dégagent seront plus pertinentes dans la lutte contre le *spamming* de dimension internationale.

[1671] Ne sont pas concernées par ce cas de figure les filiales puisqu'une société mère ne peut obtenir la réparation du préjudice subi par sa filiale, et *vice versa*, puisque chaque société du groupe étant une entité juridique autonome. – Sur cette autonomie des filiales, v. not. Cass. com., 18 mai 1999, pourvoi n° 96-19235, *inédit* (« *Mais attendu que c'est à bon droit et sans dénaturer les termes du litige que l'arrêt retient, par motifs propres et adoptés, que, sauf à méconnaître la règle que " nul ne plaide par procureur ", une société-mère ne peut se substituer à sa filiale pour intenter à ses lieu et place une action judiciaire visant à la réparation d'un préjudice personnel prenant sa source dans le préjudice subi par cette seule filiale et que la seule relation de contrôle de la société* [filiale] *par la société* [mère] *ne confère pas à celle-ci un intérêt à agir* »). – Cass. Com., 8 avr. 2008, pourvoi n° 07-10939, *inédit* (a justifié sa décision la cour d'appel qui a déclaré irrecevable l'action d'une société mère au motif que son action « *ne visait qu'à la réparation d'un préjudice prenant sa source dans celui subi par sa seule filiale* »).

§ 2. LE « SPAMMEUR » RÉSIDANT HORS DE L'UNION EUROPÉNNE

553. Lorsque le *spamming* dépasse les frontières de l'Union européenne, l'absence de règle internationale de compétence impose de revenir aux règles nationales édictées par chaque État afin de déterminer si leur juridiction est compétente. L'analyse de ces règles est particulièrement importante puisque les *spams* sont envoyés dans la majorité des cas depuis des États n'appartenant pas à l'Union européenne [1672]. Pour les besoins de cette étude, il convient donc de vérifier si les règles françaises de compétence reconnaissent la compétence des juridictions françaises. En droit français, la compétence internationale des juridictions françaises est gouvernée par le principe de la projection, sur le plan international, des règles internes de compétence territoriale. Ce principe rend applicables, par principe, les règles ordinaires de compétence (A.). Toutefois, nous verrons que, dans certaines hypothèses, des règles subsidiaires fondées sur la nationalité auront vocation à s'appliquer (B.).

A. LES REGLES ORDINAIRES DE PRINCIPE

554. Fondements et portée. La compétence internationale des juridictions françaises est déterminée selon le principe jurisprudentiel de l'extension à l'ordre international des règles françaises internes de compétence [1673]. Comme le souligne Jean-Baptiste SIALELLI, avocat à la cour d'appel de Paris, « *la formule mérite d'être retenue comme instaurant un système général de règlement des conflits de juridictions, fondé sur des éléments de rattachement étrangers à la nationalité des parties, et dans lequel les règles de compétence des articles 14 et 15 du Code civil feraient figure d'exceptions, quelle que soit l'étendue de leur application* » [1674]. À cet égard, deux dispositions d'origine interne régissent la compétence. L'une, fixée à l'article 42 alinéa 1er du Code de procédure civile (CPC), pose une règle de principe qui retient la compétence de la juridiction « *du lieu où demeure le défendeur* » [1675]. L'autre, énoncée à l'article 46 du CPC, offre au demandeur une option lui

[1672] V. *supra* : n° 74.

[1673] Cass. civ. 1re, 19 oct. 1959, *Pelassa*, *D.* 1960, jurispr., p. 37 et s., note G. Holleraux ; *Rev. crit. DIP* avr.-juin 1960, p. 215 et s., note Y. Loussouarn ; *JDI* 1960, p. 486 et s., obs. J.-B. Sialelli. – Cette formule est confirmée, trois plus tard, dans l'arrêt *Scheffel* : « *la compétence internationale se détermine par extension des règles de compétence territoriale interne* » (Cass. civ. 1re, 30 oct. 1962, *JDI* 1963, p. 1072 et s., obs. J.-B. Sialelli; *Rev. crit. DIP* janv.-mars 1963, p. 387 et s., note Ph. Francescakis ; *D.* 1963, jurispr., p. 109 et s., note G. Holleaux ; *GAJFDIP*, n° 37, p. 319 et s.). – Pierre MAYER et Vincent HEUZE, *Droit international privé*, *op. cit.*, spéc. n° 283 et s., p. 206 et s. – Marie-Laure NIBOYET et Géraud DE GEOUFFRE DE LA PRADELLE, *Droit international privé*, *op. cit.*, spéc. n° 402 et s., p. 349 et s.
Pour des applications de ce principe en matière délictuelle, v. André HUET, *Compétence des tribunaux français à l'égard des litiges internationaux*, fasc. préc., spéc. nos 37-43.

[1674] Jean-Baptiste SIALELLI, obs. sous Cass. civ. 1re, 19 oct. 1959, arrêt préc., *JDI* 1960, p. 486.

[1675] Selon l'article 43 du Code de procédure civile, « *Le lieu où demeure le défendeur s'entend : - s'il s'agit d'une personne physique, du lieu où celle-ci a son domicile ou, à défaut, sa résidence, - s'il s'agit d'une personne*

permettant en certaines matières de déroger à cette compétence de principe [1676]. En particulier, en matière délictuelle, il peut choisir de saisir, soit la juridiction « *du lieu du fait dommageable* », soit celle « *dans le ressort de laquelle le dommage a été subi* » [1677]. Transposées à l'échelle internationale, ces règles internes permettent ainsi de déclarer le juge français compétent dès lors que l'un des trois critères de rattachement est localisé sur le territoire français, à savoir : le lieu du domicile du défendeur, celui du fait générateur ou celui du dommage subi et ce, quelle que soit la nationalité des parties. En matière internationale, il est essentiel que la compétence du for du domicile du défendeur ne soit pas unique, en particulier lorsque celui-ci serait très éloigné de celui du demandeur. Si tel devait être le cas, il existerait alors de grandes chances pour que le demandeur abandonne toute action, faute d'un tribunal accessible [1678]. Comme l'explique le professeur Gabrielle KAUFMANN-KOHLER : « [l]*a compétence unique du domicile du défendeur aboutirait* […] *à des conséquences incompatibles avec l'accès effectif aux tribunaux garanti par les droits de l'homme et peut-être aussi avec l'interdiction de déni de justice du droit international général* » [1679].

555. La transposition des règles françaises au *spamming*. Appliqué au *spamming*, l'article 42 du CPC n'a pas vocation à s'appliquer dans le cadre de notre étude puisque, par hypothèse, le « spammeur » ne réside pas en France. Comme nous venons de l'exposer, il est essentiel que dans un contexte international, cette règle de compétence ne soit pas la seule applicable et à plus forte raison lorsque le litige concerne un cas de *spamming*. Pour s'en convaincre, prenons l'exemple d'une arnaque à la nigériane [1680]. Le

morale, du lieu où celle-ci est établie ». – S'agissant du domicile de la personne physique, celui-ci est défini comme le « *lieu où il a son principal établissement* » (art. 102 C. civ.). Il s'agit du lieu où elle habite effectivement en permanence ou celui où se concentre le centre principal de ses affaires. À défaut de connaître le domicile du défendeur, le lieu où demeure le défendeur s'entend, dans ce cas, de son lieu de résidence, un établissement temporaire ou épisodique (résidence secondaire ou occasionnel pour l'exercice de son activité pendant un certain temps, par exemple). Quant au domicile de la personne morale, il correspond à son siège social mentionné au Registre du Commerce et des Sociétés ou un établissement secondaire, en application de la jurisprudence, dite des « gares principales », par référence à la décision dont elle émane qui s'est appliquée aux chemins de fers. Encore connue sous le nom de « jurisprudence des sièges secondaires », elle permet d'assigner une personne morale au lieu de cet établissement secondaire, à condition que ce dernier soit pourvu d'une autonomie financière et juridique suffisante. Á défaut, l'art. 42 al. 3 C. proc. civ. énonce, dans une formulation dont on peut regretter l'imprécision, que « *si le défendeur n'a ni domicile ni résidence connus, le demandeur peut saisir la juridiction du lieu où il demeure ou celle de son choix s'il demeure à l'étranger* ». Pour clarifier cette disposition, le professeur Bernard AUDIT explique que : « *Il paraît impossible de lire ce texte comme conférant une compétence internationale aux tribunaux français en cas d'absence de domicile ou de résidence connus du défendeur en France ou à l'étranger, sans exigence de lien avec la France* » (*Droit international privé, op. cit.*, spéc. n° 344, p. 294).

[1676] Art. 46 C. proc. civ.

[1677] V. Hélène GAUDEMET-TALLON, « La compétence internationale à l'épreuve du Nouveau Code de procédure civile : aménagement ou bouleversement ? », art. préc., spéc. p. 29.

[1678] Dans un contexte plus général, V. Gabrielle KAUFMANN-KOHLER, « Internet et mondialisation de la communication », art. préc., spéc. p. 111.

[1679] Gabrielle KAUFMANN-KOHLER, art. préc.

[1680] V. *supra* : n° 107.

« spammeur » étant domicilié dans un pays africain, il appartiendrait alors au droit nigérian de déterminer s'il est possible de saisir ses juridictions nationales. Dans l'affirmative, un « spammé » résidant en France, victime de cette attaque, éprouverait ainsi les plus grandes difficultés pour engager une action en justice. L'autre inconvénient proviendrait du risque de laisser un « spammeur » impuni si celui-ci choisissait d'élire domicile dans un « paradis numérique », pour reprendre l'expression du professeur Pierre-Yves GAUTIER [1681], c'est-à-dire un État où la pratique du *spamming* n'est pas ou peu sanctionnée (« *spam harbour* » [1682]) [1683]. Il convient donc de se tourner vers l'article 46 du CPC. Selon cette disposition, les juridictions françaises sont compétentes lorsque le fait générateur ou le dommage est localisé en France. Appliqué au *spamming*, on aboutit à retenir la compétence des juridictions françaises dans deux hypothèses : en cas de dommage localisé en France ou lorsque le « spammeur », établi hors de l'Union européenne, envoie des *spams* à partir de postes situés en France. Tel pourrait être le cas lorsque ce dernier a recours à des PC Zombies localisés sur le territoire français. On rejoint ainsi la solution déjà dégagée de l'application du règlement Bruxelles I et on retrouve inéluctablement les difficultés y afférentes [1684].

B. LA REGLE DE COMPETENCE SUBSIDIAIRE

556. Le caractère subsidiaire. Lorsqu'aucun des critères de rattachement de principe – lieu du fait générateur ou celui du dommage – n'est localisé en France, la compétence internationale des juridictions françaises peut toutefois être retenue, à titre subsidiaire, sur le fondement des articles 14 et 15 du Code civil dès lors que le demandeur ou le défendeur est de nationalité française [1685].

[1681] Pierre-Yves GAUTIER, « Du droit applicable dans le « village planétaire » au titre de l'usage immatériel des œuvres », *D.* 1996, p. 131 et s., spéc. p. 132.

[1682] Par exemple, la « principauté de Sealand » située à quelques miles des côtes britanniques : Sylvain SIMONEAU, « Un paradis numérique que Londres pourrait revendiquer », disponible sur : http://www.zdnet.fr/actualites/internet/0,39020774,2060557,00.htm.

[1683] Tel pourrait être le cas, par exemple, lorsque même établis sur le territoire d'un État partie à l'un des traités, le « spammeur » choisit volontairement de s'établir là où les traités sont plus difficilement applicables en pratique (longueur des procédures ...).

[1684] Sur ces difficultés, v. *supra* : n° 555.

[1685] La Cour de cassation a jugé que l'article 14 du Code civil « *qui donne compétence à la juridiction française en raison de la nationalité française du demandeur, n'a lieu de s'appliquer que lorsqu'aucun critère ordinaire de compétence territoriale n'est réalisé en France* » (Cass. civ. 1re, 19 nov. 1985, *Orliac*, *Bull. civ.* I, n° 306, p. 271 et s. ; *Rev. crit. DIP* 1986, p. 712 et s., note Y. Lequette ; *JDI* 1986, p. 719 et s., note A. Huet). – Il est intéressant de rappeler qu'historiquement, lors de l'élaboration du Code civil, la compétence internationale était fondée sur ces seuls articles. La jurisprudence française avait pour sa part refusé pendant longtemps aux justiciables étrangers résidant en France l'accès aux juridictions françaises. Il résultait de ces deux dispositions que les juridictions françaises étaient internationalement compétentes si le demandeur (art. 14) ou le défendeur (art. 15) avait la nationalité française et la jurisprudence en avait ainsi déduit le principe de l'incompétence des

557. La nationalité française, condition nécessaire et suffisante. Sauf renonciation du demandeur aux privilèges de compétences des articles 14 et 15 précités [1686], et chaque fois que ces dispositions sont applicables, la nationalité de l'une des parties, personne physique ou personne morale, constitue la condition nécessaire et suffisante requise [1687]. La nationalité s'apprécie par référence au droit français dans la mesure où il s'agit de déterminer la compétence des tribunaux français, au jour de l'introduction de l'instance, c'est-à-dire lors de l'assignation. Transposée en matière de *spamming*, l'article 14 du Code civil permet ainsi à tout « spammé » de nationalité française et, ce même s'il réside à l'étranger, de saisir ses juridictions nationales. Toutefois, la nationalité reste un critère de rattachement secondaire ne permettant pas de surmonter les difficultés que soulèvent les deux autres critères de rattachement, à savoir fait générateur ou dommage. Cette insatisfaction nous conduit dès lors à proposer un nouveau critère de rattachement.

§ 3. PROPOSITIONS D'UN NOUVEAU CRITÈRE DE RATTACHEMENT

558. La résidence du « spammé », un rattachement stable. Afin de dépasser les critiques attachées à la localisation du lieu du fait générateur et à celle du lieu du dommage, le pays de la résidence habituelle du « spammé » pourrait apparaître comme un rattachement pertinent en matière de compétence juridictionnelle. Plusieurs arguments plaident en sa faveur. D'une part, cette solution répondrait à un souci de pragmatisme. En effet, elle permettrait de surmonter les difficultés qui découlent d'une situation où le lieu de survenance du dommage est fortuit, ce qui est très fréquent désormais en raison de la possibilité de recevoir des *e-mails* en quelqu'endroit que ce soit. Traditionnellement présentée comme « *le lieu où la personne demeure effectivement, pourvu que ce soit de manière assez stable et habituelle* » [1688], la résidence correspond non seulement à une présence physique et effective

juridictions françaises dans les litiges entre étrangers. Ce principe fut toutefois définitivement abandonné par la Cour de cassation (v. not. Cass. civ. 1re, 30 oct. 1962, *Scheffel*, arrêt préc. : « *l'extranéité des parties n'est pas une cause d'incompétence des juridictions françaises* »).

[1686] Très tôt, la Cour de cassation a considéré que l'article 14 du Code civil n'était pas d'ordre public et permettait aux Français de renoncer à son bénéfice, v. not. Cass. req., 15 nov. 1827, *S.* 1828, 1, p. 124 (sur cette renonciation, v. Bernard AUDIT, *Droit international privé*, *op. cit.*, nos 366-371, pp. 315-317. – Pierre MAYER et Vincent HEUZE, *Droit international privé*, *op. cit.*, spéc. n° 296 et s., p. 218 et s. – Marie-Laure NIBOYET et Géraud DE GEOUFFRE DE LA PRADELLE, *Droit international privé, op. cit.*, spéc. n° 397, pp. 346-374.).

[1687] Notons que les articles 14 et 15 du Code civil visent des « obligations contractées » avec un Français ou par un Français. Le terme « contracté » peut porter à confusion et laisser penser que seules les obligations découlant de la conclusion d'un contrat sont prises en compte. Or, la jurisprudence a interprété une conception extensive de cette notion permettant d'englober la matière délictuelle (v. sur ce point, Bernard AUDIT, *Droit international privé*, *ibid.*, no 360, pp. 309-310. – Pierre MAYER et Vincent HEUZE, *Droit international privé*, *ibid.*, spéc. n° 292, p. 215.).

[1688] Jean CARBONNIER, *Droit civil : Les personnes, op. cit.*, spéc. n° 55, p. 102 .

de l'intéressé en un lieu, mais aussi au lieu où sont centralisés ses intérêts [1689]. Caractérisée par une certaine permanence, significative de stabilité, la désignation de la résidence habituelle exclut ainsi toute présence de courte durée dans un lieu (par exemple, un bref séjour en vacances ou un déplacement professionnel dans un pays) et est, pour cette raison, souvent « *préférée au domicile comme impliquant une localisation plus véridique* » [1690]. D'autre part, la résidence répondrait à l'objectif procédural que poursuit la règle de conflit juridictionnelle, à savoir la garantie d'une bonne administration de la justice et l'organisation concrète du procès. L'accès à un tribunal peut être rendu plus difficile en raison de l'éloignement entre le tribunal désigné comme compétent et l'environnement familier du demandeur. Dans un souci de faciliter l'accès à la justice, il serait dès lors opportun de privilégier le caractère permanent de la résidence du demandeur plutôt qu'un lieu de survenance accidentel ou temporaire. Ce choix permettrait également de répondre à un impératif de sécurité juridique en permettant d'assurer la prévisibilité de la désignation de la juridiction compétente [1691].

559. L'hostilité actuelle de la CJCE. Malgré ses avantages (pragmatisme et souplesse), le lieu de résidence du « spammé » se heurte toutefois à la position actuelle adoptée par la CJCE en matière de compétence juridictionnelle. Celle-ci a en effet exprimé son hostilité à l'idée d'admettre que les dommages soient considérés comme ressentis dans le pays de la résidence habituelle de la victime et ce, quel que soit le lieu de leur survenance. Dans l'affaire *Marinari* [1692], le demandeur, domicilié en Italie, avait intenté une action en justice en Italie afin d'obtenir réparation du préjudice subi à la suite de son arrestation en Angleterre et de la mise sous séquestre de billets à ordre qu'il avait déposés dans une banque

[1689] V. Horatia MUIR-WATT, *Domicile et résidence dans les rapports internationaux, J.-Cl.Civil Code, Art. 102 à 111*, Fasc. unique, 2008.
[1690] Jean CARBONNIER, *Droit civil : Les personnes, op. cit., loc. cit.*
[1691] Cette solution rejoindrait ainsi les propositions formulées à l'occasion de la révision du règlement Bruxelles I qui propose, en matière de droits de la personnalité, de reconnaître la compétence des tribunaux autre que celui du lieu du domicile du défendeur dès lors qu'il existe un « *lien suffisant, substantiel ou significatif* » avec le pays dans lequel est portée l'action et sous réserve que cette désignation respecte un impératif de prévisibilité. – V. en sens, PARLEMENT EUROPEEN, Resolution on the implementation and review of Council Regulation (EC) n° 44/2001 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters, 2009/2140 (INI), du 7 septembre 2010, spéc. pt Q : " *as regards rights of the personality, there is a need to restrict the possibility for forum shopping by emphasising that, in principle, courts should accept jurisdiction only where a sufficient, substantial or significant link exists with the country in which the action is brought, since this would help strike a better balance between the interests at stake, in particular, between the right to freedom of expression and the rights to reputation and private life* ". – V. ég. COMMISSION EUROPEENNE, Proposition de règlement du Parlement européen et du Conseil concernant la compétence judiciaire, la reconnaissance et l'exécution des décisions en matière civile et commerciale (Refonte), 14 décembre 2010, COM(2010) 748 final, 2010/0383 (COD) : « *Le for du domicile du défendeur doit être complété par d'autres fors autorisés en raison du lien étroit entre la juridiction et le litige ou en vue de faciliter une bonne administration de la justice. L'existence d'un lien étroit devrait garantir la sécurité juridique en évitant que le défendeur soit attrait devant une juridiction d'un État membre qui n'était pas raisonnablement prévisible pour lui. Cet aspect est important, en particulier dans les litiges concernant les obligations non contractuelles découlant d'atteintes à la vie privée et aux droits de la personnalité, notamment la diffamation* » (considérant 12 nouveau).
[1692] CJCE, 19 sept. 1995, *Marinari*, arrêt préc.

anglaise. La défenderesse avait alors soulevé l'incompétence de la juridiction italienne au motif que le dommage qu'il avait subi ne consistait pas seulement en l'atteinte à la personne et à ses biens dont il avait souffert en Angleterre mais plus généralement résultait de la diminution de son patrimoine. La Cour suprême de cassation italienne, saisie pour résoudre à titre préalable ce problème de compétence, avait interrogé la Cour de justice de la question préjudicielle suivante : la notion de « lieu du fait dommageable » devait-elle s'entendre comme le lieu où était survenu le dommage à la personne et à des choses ou aussi comme le lieu où avaient été subis les dommages patrimoniaux ? La CJCE s'était prononcée en faveur de la première branche de l'alternative. Elle avait précisé que le seul lieu à prendre en compte était celui où se réalisait la première manifestation matérielle du dommage éprouvé par la victime au moment où l'évènement causal s'était réalisé : « [l]*a notion de " lieu où le fait dommageable s'est produit ",* [figurant à l'article 5.3° du règlement n° 44/2001] *doit être interprétée en ce sens qu'elle ne vise pas le lieu où la victime prétend avoir subi un préjudice patrimonial consécutif à un dommage initial survenu et subi par elle dans un autre État contractant* » [1693]. Au soutien de sa réponse, la Cour a ainsi énoncé que cette notion « *ne saurait être interprétée de façon extensive au point d'englober tout lieu où peuvent être ressenties les conséquences préjudiciables d'un fait ayant causé un dommage effectivement survenu dans un autre lieu* » [1694]. Cette interprétation de l'article 5.3 précité a été, par la suite, confirmée dans l'arrêt *Khronhofer* du 10 juin 2004 [1695]. La CJCE, s'appuyant de la solution dégagée de l'arrêt *Marinari* [1696], a en effet exclu que l'expression « *lieu où le fait dommageable s'est produit* » de l'article 5.3 vise le lieu du domicile du demandeur, là « *où serait localisé " le centre de son patrimoine " au seul motif qu'il y aurait subi un préjudice*

[1693] CJCE, 19 sept. 1995, arrêt préc., spéc. pt 21 et dispositif.

[1694] CJCE, 19 sept. 1995, arrêt préc., spéc. pt 14. – V. ég. CJCE 11 janv. 1990, *Sté Dumez*, arrêt préc. (à propos des victimes indirectes, la Cour a jugé que « *la règle de compétence juridictionnelle énoncée à l'article 5, point 3, de la Convention du 27 septembre 1968* […] *ne peut être interprétée comme autorisant un demandeur qui invoque un dommage qu'il prétend être la conséquence d'un préjudice subi par d'autres personnes, victimes directes du fait dommageable, à attraire l'auteur de ce fait devant les juridictions du lieu où il a lui-même constaté le dommage dans son patrimoine* ».

[1695] CJCE, 10 juin 2004, aff. C-168/02, *Rudolf Kronhofer, D.* 2005. pan., p.1268, obs. P. Courbe et H. Chanteloup ; *Rev. crit. DIP* avr.-juin 2005, p. 326 et s., note H. Muir Watt (en l'espèce, un épargnant domicilié en Autriche avait transféré une somme d'argent sur un compte de placement en Allemagne après avoir été incité par téléphone par une société de placement dont le siège était situé en Allemagne. Les opérations spéculatives à la bourse de Londres avait entrainé la perte d'une partie de la somme transférée par cet épargnant qui avaient conduit ce dernier à assigner la société de placement et ses gérants devant les juridictions autrichiennes pour ne pas l'avoir suffisamment informé des risques que comportait cette opération. Les juridictions autrichiennes du premier et du second degré s'étaient déclarées incompétentes pour connaître du litige sur le fondement de l'article 5.3 au motif que le tribunal du lieu du domicile ne serait pas celui « du lieu où le fait dommageable s'est produit » dans la mesure où ni le lieu du fait générateur ni celui du dommage ne seraient situés en Autriche. La CJCE avait donc été saisie d'une question préjudicielle aux fins de déterminer si l'expression « lieu du fait dommageable s'est produit » devait être interprétée largement pour permettre, en cas de préjudice purement patrimonial, d'englober le lieu du domicile du demandeur où est également localisé le centre de se patrimoine).

[1696] CJCE, 19 sept. 1995, arrêt préc.

financier résultant de la perte d'éléments de son patrimoine intervenue et subie dans un autre État contractant » [1697].

560. Une évolution possible de la CJCE ? Malgré la position actuelle de la CJCE, une évolution future pourrait être espérée au regard de la position qu'elle a récemment adoptée en matière contractuelle. En effet, à l'occasion de l'arrêt *Wood Flour* [1698], elle a assoupli l'interprétation du critère de proximité. En l'espèce, la CJCE a admis qu'« *en cas d'impossibilité de déterminer le lieu de la fourniture principale des services sur la base tant des dispositions du contrat lui-même que de son exécution effective* [article 5.1 du règlement n° 44/2001 [1699]] *il convient d'identifier ce lieu d'une autre manière qui respecte à la fois les objectifs de prévisibilité et de proximité poursuivis par le législateur* » [1700]. À cette fin, la Cour a retenu « *comme lieu de la fourniture principale des services fournis par un agent commercial, le lieu où cet agent est domicilié* ». Elle a justifié son choix en précisant que « *ce lieu est toujours susceptible d'être identifié avec certitude et donc prévisible* » et a ajouté que celui-ci « *présente un lien de proximité avec le litige dès lors que l'agent y fournira, selon toute probabilité, une partie non négligeable de ses services* » [1701]. Bien que cette décision ait été rendue en matière contractuelle, cette interprétation large de la proximité pourrait laisser présager, à l'avenir, une évolution similaire en matière délictuelle. Dans le domaine précis du *spamming*, il serait intéressant de retenir l'existence de liens non négligeables avec la résidence du « spammé » puisque la CJCE prend elle-même cette liberté avec la notion de proximité. Certes, il pourrait toujours être reproché à ce correctif de malmener l'orthodoxie de la règle de compétence du lieu de survenance du dommage proprement dit mais cette solution gagnerait en prévisibilité, vertu qu'il est impératif de préserver.

*

* * *

561. Le règlement Bruxelles I permet, lorsque le « spammeur » réside dans l'Union européenne, de désigner, dans les hypothèses les plus simples, soit la juridiction du lieu du

[1697] CJCE, 10 juin 2004, arrêt préc., spéc. pt 21.
[1698] CJCE, 11 mars 2010, aff. C-19/09, *Wood Floor Solutions Andreas Domberger GmbH v. Silva Trade SA*, *JCP* 2010, éd. E., alerte 1579, note M. Fernet.
[1699] Règl. (CE) n° 44/2001 préc. – L'article 5.1 du règl. n° 44/2201 dispose que « *le lieu d'exécution de l'obligation qui sert de base à la demande est : - pour la fourniture de services, le lieu d'un État membre où, en vertu du contrat, les services ont été ou auraient dû être fournis* ».
[1700] CJCE, 11 mars 2010, aff. préc., spéc. point 41.
[1701] *Id.*, spéc. point 42.

fait générateur, à savoir celle du lieu d'émission du message, soit la juridiction du lieu du dommage, c'est-à-dire celle du lieu de sa réception qui coïncidera le plus souvent avec le lieu de résidence du « spammé ». Toutefois, dans des cas plus complexes, ce règlement n'offre pas de réponses convaincantes. D'une part, en cas de dissociation entre le lieu d'émission et celui de résidence du « spammeur », aucune solution clairement établie ne se dégage. D'autre part, en cas de scission entre le lieu de réception et le lieu de résidence du « spammé », le choix de la compétence de la juridiction du lieu du dommage n'apparaît pas judicieux en raison des difficultés inhérentes à sa localisation, celui-ci pouvant varier au grès des déplacements du destinataire. Lorsque le « spammeur » est établi hors de l'Union européenne, les solutions offertes par les règles de conflits françaises aboutissent à des conclusions analogues. L'impossibilité d'aboutir à des réponses complètes et pertinentes dans les cas de *spamming* les plus complexes conduit à espérer une évolution des règles de conflits classiques en créant un chef de compétence particulier en matière de *spamming*. Cette proposition reviendrait à localiser fictivement le lieu de survenance du dommage au lieu de résidence habituelle du « spammé », lieu où sont concentrés les intérêts du destinataire des messages. Elle correspondrait en effet au lieu où il exerce son droit de jouir librement et pleinement des services de messagerie (envoi et réception de messages) et plus largement, de son droit fondamental d'accéder aux services de communication au public en ligne et donc là où ses droits sont lésés [1702].

[1702] « [L]*a liberté de communication et d'expression, énoncée à l'article 11 de la Déclaration des droits de l'homme et du citoyen de 1789, fait l'objet d'une constante jurisprudence protectrice par le Conseil constitutionnel* […] *Cette liberté implique aujourd'hui, eu égard au développement généralisé d'internet et à son importance pour la participation à la vie démocratique et à l'expression des idées et des opinions, la liberté d'accéder à ces services de communication au public en ligne* » (Cons. const., DC n° 2009-580 du 10 juin 2009).

SECTION II. LES CONFLITS DE LOIS OCCASIONNÉS PAR LE *SPAMMING*

562. Quid de la loi compétente applicable ? Une fois que le « spammé » connaît la juridiction compétente, il convient de déterminer la loi applicable pour résoudre le litige en cause. Rappelons au préalable que le *spamming*, à chacun des stades de son processus (collecte puis envoi), peut consister en une faute civile délictuelle à l'origine d'un dommage et/ou une atteinte à un droit de la personnalité (droit sur les données à caractère personnel droit à la tranquillité) [1703]. Cette distinction est importante dans la mesure où en droit international privé, les règles de conflit de lois applicables en matière délictuelle (§ 1.) et celles régissant les droits de la personnalité (§ 2.) n'aboutissent pas nécessairement à la désignation d'une loi identique. En l'absence de hiérarchie entre les lois désignées comme compétentes, un même litige pourrait ainsi être régi par deux lois nationales différentes. Cette situation risque d'engendrer des difficultés inextricables, en particulier lorsque la mise en œuvre de ces lois aboutit à des solutions divergentes. Pour éviter de telles conséquences, nous nous attacherons à la recherche d'une règle de conflit unique (§ 3.).

§ 1. LA LOI APPLICABLE AUX DÉLITS COMMIS PAR LES « SPAMMEURS »

563. Comme il a été indiqué à titre préliminaire, dans les hypothèses qui nous intéressent, le *spamming* relève de la sphère extracontractuelle [1704]. En matière délictuelle, c'est le règlement n° 864/2007 sur la loi applicable aux obligations non contractuelles, dit règlement « Rome II » [1705], adopté le 11 juillet 2007, qui établit à l'échelle européenne les règles de conflit de lois. Il convient au préalable de vérifier si le *spamming* entre dans le

[1703] V. *supra :* n° 169 et s.
[1704] V. *supra* : 537.
[1705] Règl. (CE) n° 864/2007 du Parlement européen et du Conseil sur la loi applicable aux obligations non contractuelles du 11 juillet 2007, J.O.U.E. n° L 199 du 31 juillet 2007, p. 40 et s. – Pour une présentation générale du règlement Rome II, v. par ex. Carine BRIERE, « Le règlement (CE) n° 864/2007 du 11 juillet 2007 sur la loi applicable aux obligations non contractuelles (" Rome II "), *JDI* 2008, doctr., p. 31 et s. – Frédéric GUERCHOUN et Stéphane PIEDELIEVRE, « Le règlement sur la loi applicable aux obligations non contractuelles (" Rome II ") », *Gaz. Pal.* 21-23 et 28-30 oct. 2007, p. 3107 et s. – Thomas KADNER GRAZIANO, « Le nouveau droit international privé communautaire en matière de responsabilité extracontractuelle (règlement Rome II) », *Rev. crit. DIP* juill.-sept. 2008 p. 445 et s. – Gérard LEGIER, « Le règlement " Rome II " sur la loi applicable aux obligations non contractuelles », *JCP* 2007, éd. G., I. 207. – Pierre MAYER et Vincent HEUZE, *Droit international privé,* 9e éd., Montchrestien, 2007, spéc. n° 679 et s., p. 510 et s. – Louis D'AVOUT et Tristan AZZI (présenté par), « Le règlement n° 864/2007 du 11 juillet 2007 sur la loi applicable aux obligations non contractuelles, dit " Rome II " », *D.* 2009, dossier, p. 1619 et s. – Dans ce dossier, voir lire différentes contributions : Tristan AZZI, « Bruxelles I, Rome I, Rome II : regard sur la qualification en droit international privé communautaire », *id.,* p. 1621 et s. – Louis d'AVOUT, « Que reste-t-il du principe de territorialité des faits juridiques ? (une mise en perspective du système Rome II), p. 1629 et s. – Olivera BOSKOVIC, « L'autonomie de la volonté dans le règlement Rome II », *id.,* p. 1639 et s. – Édouard TREPPOZ, « La lex loci protectionis et l'article 8 du règlement Rome II », *id.,* p. 1643 et s. – Louis PERREAU-SAUSSINE, « Les mal-aimés du règlement Rome II : les délits commis par la voie des médias », *id.,* p. 1647 et s.

champ d'application dudit règlement (§. A.) et dans l'affirmative, d'étudier en pratique sa mise en œuvre (§. B.)

A. L'APPLICATION DU REGLEMENT ROME II AU *SPAMMING*

564. Un règlement très attendu. Avant 2007, faute de consensus, il n'existait aucune règle substantielle ni aucune règle de conflit internationale ou régionale réglant la question de la loi applicable à la responsabilité civile délictuelle ou quasi délictuelle [1706]. Jusqu'à cette date, coexistaient seulement des conventions internationales portant sur des cas spécifiques de responsabilité délictuelle[1707] et des lois nationales des États, dont la diversité favorisait les risques de *forum shopping* [1708]. Face à l'accroissement des délits complexes, la nécessaire création d'une règle de conflit commune aux États membres s'imposait afin de permettre la désignation de la loi applicable. À l'issue d'une longue période de procédure et de négociations [1709], le Parlement européen adopta, le 11 juillet 2007, le règlement Rome II relatif à la détermination de la loi applicable en matière extracontractuelle [1710]. La portée de ce règlement est incontestable dans la mesure où ce dernier s'impose dans tous les États membres, à l'exception du Danemark [1711]. Son importance se vérifie également au regard des règles de conflit qu'il fixe puisque ces dernières, se substituant aux différents droits nationaux, deviennent les seules règles de conflit applicables dans les États membres, dans les domaines couverts par le règlement [1712]. Répondant à un souci de pragmatisme, cette solution apparaît opportune : la coexistence des règles de conflit d'origine communautaire applicables aux litiges intra-communautaires et celles d'origine nationale régissant les litiges de nature extracommunautaire, aurait inéluctablement compromis l'objectif d'harmonisation

[1706] À l'inverse, les États membres ont très tôt abouti à un accord sur les règles de conflit applicables en matière contractuelle. La Convention de Rome de 1980 avait en effet permis l'adoption de règles de conflit uniformes destinées à désigner la loi applicable aux obligations contractuelles.

[1707] Par exemple, la Convention de la Haye du 4 mai 1971 relative à la loi applicable en matière d'accident de la circulation routière ou la Convention de la Haye du 2 octobre 1973 sur la loi applicable à la responsabilité du fait des produits défectueux.

[1708] C'est-à-dire une « *fraude aux lois étrangères* » et qui consiste en « *la recherche par les particuliers dans l'ordre international d'une autorité complaisante* […] *en vue d'obtenir ce qui ne pourrait l'être selon la loi applicable* » (Bernard AUDIT, *Droit international privé*, *op. cit.*, spéc. n° 261, pp. 227-228).

[1709] Pour une description très complète du processus d'élaboration du règlement et des difficultés de consensus, v. Gérard LEGIER, « Le règlement " Rome II " sur la loi applicable aux obligations non contractuelles », chron. préc., spéc. n^{os} 3-7.

[1710] règl. (CE) n° 864/2007 préc.

[1711] Art. 1 § 4 et Consid. 40 règl. (CE) n° 864/2007 préc.

[1712] Toutefois, en raison de son caractère très récent, peu de jurisprudence existe en la matière et permettant de donner une ligne directrice aux juges pour appliquer ce règlement. Par conséquent, si le règlement Rome II marque une nouveauté par rapport aux solutions dégagées par la jurisprudence française, il ne s'en dégage pas totalement. Les solutions jurisprudentielles françaises conservent ainsi leur intérêt puisqu'elles permettront de faciliter l'interprétation de ces règles communautaires.

et accru les « *risques de distorsion entre les justiciables de la Communauté* » [1713]. Ainsi, la qualité de neutralité que l'on prête souvent à la règle de conflit prend ici encore davantage de sens puisque la loi désignée par le règlement s'applique, que cette dernière soit celle d'un État membre ou celle d'un État tiers : c'est l'application « universelle » dans les États membres [1714].

565. Conditions d'application. La mise en œuvre du règlement Rome II est soumise au respect de deux conditions cumulatives : l'une temporelle et l'autre matérielle.

566. Condition temporelle. Aux termes de l'article 31, le règlement s'applique « *aux faits générateurs de dommages survenus après son entrée en vigueur* ». De façon explicite, le critère temporel de référence doit s'entendre comme le fait générateur. Or, s'agissant de la date d'entrée en vigueur du règlement Rome II, aucune disposition n'apporte de précision sur ce point. En effet, contre toute attente, l'article 32 précise seulement la date de son application, à savoir le 11 janvier 2009. Pour pallier ce défaut rédactionnel et donner une cohérence au texte, le professeur Gérard LEGIER préconise de retenir la date d'application fixée par l'article 32 comme celle de son entrée en vigueur [1715]. C'est la solution qui nous semble également la plus raisonnable et à laquelle nous nous référerons.

567. Condition matérielle. Selon l'article 1.1, le règlement a vocation à s'appliquer « *dans les situations comportant un conflit de lois, aux obligations non contractuelles relevant de la matière civile et commerciale* » [1716], excluant notamment de façon expresse, les obligation non contractuelles découlant d'atteintes à la vie privée et aux droits de la personnalité [1717], y compris la diffamation [1718]. Trois éléments doivent donc être

[1713] Consid. 13 règl. (CE) n° 864/2007 préc.
[1714] Art. 3 règl. (CE) n° 864/2007 préc. – On retrouve cette disposition en matière contractuelle à l'article 2 de la Convention de Rome de 1980.
[1715] Sur ces difficultés, v. Gérard LEGIER, « Le règlement " Rome II " sur la loi applicable aux obligations non contractuelles », chron. préc., spéc. n° 8.
[1716] En sont notamment exclues les matières fiscales, douanières, administratives, à l'instar du règlement Bruxelles I ainsi que la responsabilité encourue par l'État pour les actes d'omission commis dans l'exercice de la puissance publique (article 1.1 règl. (CE) n° 864/2007 préc.). De même, sont exclus de son champ d'application : les obligations non contractuelles découlant de relations de famille, des régimes matrimoniaux ; celles nées de l'effet de commerce (lettres de change, de chèques, de billets à ordre) et autres instruments négociables, celles liées au droit des sociétés, associations et personnes morales, des relations entre les constituants, le trust créé volontairement, celles résultant d'un dommage nucléaire, ou encore celles découlant d'atteintes à la vie privée et aux droits de la personnalité, y compris la diffamation (article 1.2 règl. préc.). Enfin, selon l'article 1.3, le règlement n'est applicable ni à la preuve ni à la procédure
[1717] Cette exclusion du règlement Rome II justifie que l'on traite la question de l'atteinte aux droits de la personnalité en matière de *spamming* dans un développement spécifique (pour des précisions sur ces exclusions, en particulier sur celles concernant les obligations découlant d'atteintes à la vie privée et aux droits de la personnalité, v. Gérard LEGIER, « Le règlement " Rome II " sur la loi applicable aux obligations non contractuelles », chron. préc., spéc. n^{os} 14-17).
[1718] Art. 1.2 g) règl. (CE) n° 864/2007 préc.

réunis. Tout d'abord, le texte vise les « *situations comportant un conflit de lois* » [1719], c'est-à-dire qu'il s'applique à « *des situations qui comportent un ou plusieurs éléments d'extranéité par rapport à la vie sociale interne d'un pays et qui donnent vocation à s'appliquer à plusieurs systèmes juridiques* » [1720]. En outre, le règlement précise qu'il ne couvre que « la matière civile et commerciale », ce qui fait écho au domaine couvert par le règlement Bruxelles I applicable en matière de conflit de juridictions. Enfin, le règlement est applicable aux seules « obligations non contractuelles », entendues très largement comme toute obligation ne découlant pas d'un contrat mais d'un fait juridique. Pour surmonter les divergences entre les conceptions nationales entourant la notion d'« obligations non contractuelles », le règlement spécifie que cette dernière doit être entendue comme un « concept autonome » [1721] et couvre « *toute demande qui vise à mettre en jeu la responsabilité d'un défendeur et qui ne se rattache pas à la " matière contractuelle "* » [1722]. Il semble toutefois que cette autonomie apparaît très relative puisque l'on retrouve les catégories connues en droit français, à savoir les cas de responsabilité civile extracontractuelle (délits et quasi-délits), y compris ceux de responsabilité objective [1723], et les quasi-contrats [1724]. Le champ du règlement est donc très large, le dommage étant défini par l'article 2.1 comme « *toute atteinte résultant d'un fait dommageable* » [1725]. Le large rayonnement du règlement se vérifie à la lecture de l'article 2.2 qui, prenant en compte l'essor croissant du principe de précaution en droit de la responsabilité civile, énonce que le règlement « *s'applique également aux obligations non contractuelles susceptibles de survenir* », c'est-à-dire aux actions préventives [1726]. La conséquence de cette précision est

[1719] Art. 1.1 règl. (CE) n° 864/2007 préc. – V. déjà en ce sens Convention de Rome de 1980 sur la loi applicable aux obligations contractuelles (version consolidée), J.O.U.E. C. 27 du 26 janvier 1998, p. 34 et s. – Pour des précisions sur ce champ spatial du règlement Rome II, v. Frédéric GUERCHOUN et Stéphane PIEDELIEVRE, « Le règlement sur la loi applicable aux obligations non contractuelles (" Rome II ") », art. préc., spéc. n° 7, p. 3108 et s.

[1720] COMMISSION EUROPEENNE, Proposition de règlement du Parlement européen et du Conseil sur la loi applicable aux obligations non contractuelles, 22 juillet 2003, COM (2003) 427 final, p. 9.

[1721] Consid. 11 règl. n° 864/2007 préc. – V. Mathias AUDIT, « L'interprétation autonome du droit international privé communautaire », art. préc.

[1722] CJCE, 27 sept. 1988, *Kalfelis*, arrêt préc.

[1723] Consid. 11 règl. (CE) n° 864/2007 préc.

[1724] Entrent dans le champ de ce règlement les quasi-contrats, à savoir : l'enrichissement sans cause, le paiement de l'indû et la gestion d'affaires (art. 10 et 11 règl. n° 864/2007 préc.). – Sur ces notions, v. par ex. Philippe DELEBECQUE, *Droit des obligations : Contrat et quasi-contrat*, tome 1, 4e éd., Litec, coll. *Objectif droit cours*, 2007. – Il convient également d'ajouter à cette liste la *culpa in contrahendo* définie à l'article 12 comme « *l'obligation non contractuelle découlant de tractations menées avant la conclusion du contrat* ». Celle-ci correspondrait, dans le système français, à la faute commise lors de la phase de pourparlers (rétractation abusive d'une offre, refus de conclure un contrat alors même que le futur contractant a fait croire à l'autre pendant toute la période de négociations que le contrat serait conclu) qui engage la responsabilité délictuelle de son auteur. Cette faute illustre parfaitement les divergences qui peuvent exister entre les systèmes nationaux. En effet, par exemple, le droit allemand, contrairement au droit français, sanctionne cette faute sur le fondement de la responsabilité contractuelle.

[1725] Art. 2.1 règl. (CE) n° 864/2007 préc.

[1726] Sur le développement du principe de précaution en droit de la responsabilité civile, v. Mathilde BOUTONNET, *Le principe de précaution en droit de la responsabilité civile*, tome 444, L.G.D.J., 2005. – On retrouve également cette même technique d'élargissement du champ d'application aux obligations préventives en matière

contenue à l'article 2.3 au terme duquel toutes les fois où le fait générateur ou le *dommage est visé par le règlement, l'un ou l'autre doit également s'entendre comme celui « susceptible de se produire* ».

568. Application en matière de *spamming.* Transposée à la pratique du *spamming*, la condition temporelle ne pose aucune difficulté puisque seuls sont concernés les faits générateurs, c'est-à-dire les envois de *spams* survenus après son entrée en vigueur. Il en va de même de la condition matérielle puisque d'une part, en l'absence de tout lien contractuel entre les intéressés [1727], les « spammés » qui subissent un dommage à la suite de la réception de *spams,* cherchent à engager la responsabilité délictuelle du « spammeur ». D'autre part, la finalité commerciale, politique, caritative de nombreux *spams* les fait entrer sans conteste dans le champ d'application du règlement. La question de la loi applicable aux litiges nés du *spamming* sera donc tranchée en application du règlement Rome II dès lors que le litige est soumis aux juridictions françaises [1728]. Il convient donc à présent d'analyser la mise en œuvre dudit règlement en matière de *spamming* afin de déterminer selon les règles de conflit communautaires, quelle loi a vocation à trancher le litige.

B. LA MISE EN ŒUVRE DU REGLEMENT EN MATIERE DE *SPAMMING*

569. Un fonctionnement hiérarchisé des règles de conflits. L'article 4 qui permet de déterminer de façon générale la loi applicable « *aux faits dommageables* », comporte en réalité trois règles distinctes. Le premier alinéa confère une compétence de principe à la loi du lieu de survenance du dommage (1.). Dans certaines hypothèses, cette solution peut toutefois se révéler inadaptée à l'espèce à laquelle elle a vocation à s'appliquer. C'est précisément pour éviter toute situation de blocage qui résulterait d'une application trop rigide de ce rattachement, que le règlement Rome II prévoit deux exceptions. La première énonce, qu'en cas de résidence habituelle commune des parties résidentes, c'est la loi de ce pays qui doit primer [1729]. La seconde prévoit une clause d'exception qui a pour effet d'évincer

juridictionnelle, à l'article 5.3 du règlement Bruxelles I qui autorise à saisir le tribunal du lieu où le fait dommageable risque de se produire (v. *supra.*). – En matière de *spamming*, l'action préventive n'est toutefois pas pertinente puisque la simple collecte ne peut être analysée en un acte préparatoire du *spamming*. Si tel devait être le cas, toute collecte de données à caractère personnel serait alors considérée comme illicite dès l'origine. Cette affirmation reviendrait alors à remettre en cause le principe même de l'internet et en particulier, celui de la libre circulation des données sur l'internet.

[1727] V. *supra* : n° 537.

[1728] La saisine d'une juridiction d'un État entrainant l'application des règles de conflit de lois de ce même État par le juge saisi du litige.

[1729] Le principe général de l'article 4 s'applique sous réserve que les parties ne résident pas dans le même pays (art. 4 al. 2 règl. (CE) n° 864/2007 préc. : « *lorsque la personne dont la responsabilité est invoquée et la*

exceptionnellement les deux lois précitées dès lors que la situation en cause présente des liens manifestement plus étroits avec un autre pays (2.).

1. Un rattachement de principe : la loi du lieu du dommage

570. Un principe clairement établi. Sans exclure totalement de son système de règlement des conflits la loi du lieu du délit (*lex loci delicti*) [1730], le texte européen s'est néanmoins clairement prononcé en faveur de la loi du lieu « *où le dommage survient* » (*lex loci damni*), comme en témoigne son article 4, alinéa 1er : « *la loi applicable à une obligation non contractuelle résultant d'un fait dommageable est celle du pays où le dommage survient, quel que soit le pays où le fait générateur du dommage se produit et quels que soient le ou les pays dans lesquels les conséquences indirectes de ce fait surviennent* » [1731]. Afin d'assurer la sécurité juridique des solutions, les rédacteurs du règlement ont pris soin d'apporter deux précisions. D'une part, la loi compétente en matière délictuelle est celle du lieu du dommage, « *quel que soit le pays où le fait générateur du dommage se produit* ». Cette règle exclut ainsi toute possibilité de désigner la loi du lieu du fait générateur. D'autre part, le dommage doit s'entendre du seul dommage direct [1732], toute conséquence indirecte qui pourrait en découler et survenir dans un autre pays est donc indifférente. La fermeté de cette disposition est parfaitement opportune puisqu'en concentrant le lieu du dommage au lieu où s'est produit le préjudice initial, cela permet d'assurer la cohésion des décisions à intervenir. À défaut, on pourrait en effet aboutir à des solutions totalement incohérentes. Il en serait ainsi, par exemple, lorsque la victime du dommage par ricochet pourrait obtenir réparation selon la loi du lieu où celle-ci a ressenti le dommage alors que toute indemnisation lui serait refusée en application de la loi du lieu où le dommage initial est survenu. C'est

personne lésée ont leur résidence habituelle dans le même pays au moment de la survenance du dommage, la loi de ce pays s'applique »). – Cette dérogation ne sera pas développée dans la présente étude qui concerne l'hypothèse où le « spammeur » réside hors du territoire français et le « spammé » en France.

[1730] Avant le règlement Rome II, une tendance générale se dessinait déjà dans les droits européens et étrangers (États-Unis, Chine, notamment), vers un infléchissement du principe de la *lex loci delicti*, celui-ci se trouvant fortement concurrencée par la loi du lieu de résidence commune des parties et parfois par la loi du pays de la nationalité commune des parties (sur ce point, v. Hélène GAUDEMET-TALLON, *Le pluralisme en droit international privé : Richesses et faiblesses*, recueil préc., spéc. n° 208, pp. 218-219). – Dans les droits européens, v. ég. Y. LOUSSOUARN, P. BOUREL et P. DE VAREILLES-SOMMIERES, *Droit international privé,* 9e éd., *Dalloz,* 2007, n° 180-1 et 180-2, p. 225 et s.).

[1731] En faveur de cette solution, le doyen BATIFFOL souligne que « *d'une manière générale, le droit international privé tend à localiser les rapports de droit par ceux de leurs éléments qui se manifestent extérieurement, donc de préférence matériellement parce que l'intérêt des tiers, qui représente l'intérêt commun, but du droit, s'en trouve assuré et que la solution est déterminée avec plus de certitude* […]. *Il semble donc préférable d'appliquer la loi du dommage* » (A. WEILL, *Un cas épineux de compétence législative : le cas de la dissociation entre le fait générateur et le préjudice* », *in Mélanges offerts à Jacques Maury*, tome 1, Dalloz-Sirey, 1960, spéc. p. 553-554).

[1732] V. déjà en ce sens en matière juridictionnelle, CJCE, 19 sept. 1995, aff. C-364/93, *Antonio Marinari*, aff. préc. (la CJCE, statuant, à propos de l'article 5.3 de la Convention de Bruxelles du 27 septembre 1968, et reprise par le règlement Bruxelles I, avait retenu seulement le lieu de survenance de la conséquence initiale).

ainsi que la Cour de cassation française a jugé que « *s'agissant du préjudice moral subi par les victimes par ricochet, qui est en relation directe avec le fait dommageable et qui trouve sa source dans le dommage causé à la victime, la loi applicable à la réparation est celle du lieu où le dommage s'est réalisé et non celui où ce préjudice moral est subi* » [1733].

571. Justifications de la règle de principe. Cette solution de principe se recommandait non seulement en raison de motifs théoriques mais aussi de justifications d'ordre pratique. S'agissant des premiers, la préférence donnée à la *lex loci damni* apparaît en cohérence avec la finalité traditionnelle de la responsabilité délictuelle, orientée vers le dogme de la réparation [1734]. En effet, la responsabilité civile a pour finalité de permettre à la victime d'obtenir, autant que possible, une indemnisation lui permettant de se retrouver dans la situation dans laquelle il était avant la survenance du dommage. Par ailleurs, d'un point de vue pratique, le choix en faveur d'un critère de rattachement fixe et uniforme est justifié par la volonté de garantir au mieux la sécurité juridique et l'harmonisation entre les États membres, ce que ne pouvait assurer la disparité des règles nationales en la matière [1735].

572. Une réponse univoque en cas de dissociation géographique des éléments constitutifs du délit. En favorisant ce critère de rattachement, le règlement évacue ainsi toute hésitation possible en cas de dispersion géographique du fait générateur et du dommage [1736]. L'apport du règlement Rome II est donc sur ce point considérable. En effet,

---

[1733] Cass. civ. 1re, 28 oct. 2003, *Pays Fourvel c/ Sté Axa courtage et al.*, *Rev. crit. DIP* janv.-mars 2004, p. 83 et s., note D. Bureau ; *JDI* 2004, p. 499 et s., note G. Légier ; *JCP* 2004, G., II. 10006, note G. Lardeux (en l'espèce, une excursion sur le fleuve du Mékong avait été proposée au cours d'un voyage organisé au Cambodge pour un groupe de touristes français et s'était terminée tragiquement par la noyade de certains de passagers. Dans un attendu très explicite, la Cour de cassation a jugé que « *l'arrêt attaqué ayant relevé que le fait générateur du dommage était l'embarquement des passagers à bord d'un bateau instable, doté d'installations inadéquates et d'un barreur inexpérimenté, ce fait s'étant produit au Cambodge, pays où le bateau avait chaviré et celui où le dommage s'était réalisé, en appliquant la loi cambodgienne à la réparation du préjudice des victimes par ricochet, la cour d'apple a fait une exacte application de la règle de conflits de lois* »). – Rappr. CJCE 11 janv. 1990, *Sté Dumez*, arrêt préc.

[1734] En effet, aujourd'hui le droit de la responsabilité civile est tourné vers la réparation et non plus vers la répression même si une tendance inverse tend à s'imposer dans certaines hypothèses (v. *supra :* 479 et s.). – À cet égard, A. WEILL, « *la responsabilité civile est axée sur la réparation du préjudice et la protection de la victime ; on voit se développer les présomptions de responsabilité, voire les cas de responsabilité sans faute, mais on ne conçoit pas de responsabilité sans préjudice* » (*Un cas épineux de compétence législative en matière de responsabilité délictuelle : dissociation de l'acte générateur de responsabilité et du lieu du préjudice. Le dommage devient ainsi l'élément primordial de la responsabilité délictuelle et, à cet égard, paraît être un élément de localisation préférable au fait générateur de responsabilité* » (*op. cit*., spéc. p. 553). *L'élément essentiel de localisation est donc celui du dommage causé, c'est là que l'acte illicite se réalise, que le rapport de droit se noue* » (*op. cit*., spéc. p. 555). Le dommage apparaît donc comme indispensable au déclenchement de l'action en responsabilité : « *le dommage est le point de départ de l'intervention du droit civil et la réparation en est son aboutissement* » (Henri BATIFFOL, *Aspects philosophiques du droit international privé*, Dalloz, coll. *Philosophie du droit*, 1956, spéc. n° 107, p. 239). – Le règlement rappelle également cette relation entre le rattachement à la loi du lieu de survenance du dommage et « *la conception moderne du droit de la responsabilité civile* » (considérant 16 du règl. (CE) n° 864/2007 préc.).

[1735] Considérant 15 du règl. (CE) n° 864/2007 préc.

[1736] Sur cette question, v. A. WEILL, *Un cas épineux de compétence législative en matière de responsabilité délictuelle*, *op. cit*., spéc. p. 545 et s.

avant son adoption, cette question avait donné lieu à un large éventail de solutions divisant les États membres [1737]. Il ressortait ainsi des lois et de la jurisprudence une extrême diversité des solutions envisagées : certaines privilégiaient la loi du lieu du dommage tandis que d'autres favorisaient la loi du lieu du fait générateur, ou encore celle du lieu où le fait dommageable s'est produit qui pouvait alors s'entendre aussi bien comme le lieu du fait générateur que celui du dommage. Certaines règles de conflit nationales retenaient pour leur part la loi la plus favorable à la victime ou lui offraient une option [1738]. Fidèles à l'objectif de prévisibilité et de sécurité juridique, les auteurs du règlement ont donc préféré un rattachement fixe plutôt qu'un système alternatif ou optionnel [1739]. L'exclusion de cette dernière possibilité mérite, selon nous, approbation en ce sens que l'octroi d'un choix à la victime est source d'imprévisibilité. En matière de *spamming* par exemple, le « spammé » apparaîtrait ainsi nettement favorisé par rapport au « spammeur » qui resterait dans l'incertitude dans les premiers temps de l'instance. Enfin, d'un point de vue pratique, la compétence du lieu du dommage présente plusieurs avantages qui expliquent que la *lex loci damni* ait reçu les faveurs de la doctrine française avant même l'avènement du règlement Rome II [1740]. D'une part, le lieu où le dommage est constaté est souvent plus simple à identifier que celui du fait générateur puisqu'il permet de matérialiser le délit. D'autre part, entre le lieu du fait générateur et celui du dommage, il semble que c'est au lieu de la survenance du dommage que se manifeste le plus clairement là où l'équilibre des intérêts en présence a été rompu [1741]. Enfin, coïncidant le plus souvent avec celui du domicile du demandeur, il viendra pallier l'inconvénient de l'éloignement du fait générateur, tout en accélérant le processus d'indemnisation de la victime.

573. Les incidences en matière de *spamming* et propositions de rattachement. L'opportunité de cette solution se vérifie en matière de *spamming*. En effet, alors que la localisation de l'envoi des *spams* est particulièrement difficile à déterminer, notamment dans les hypothèses où le « spammeur » a recours des PC zombies ou à des adresses usurpées, le lieu du dommage est plus simple à identifier puisqu'il se confond souvent avec leur lieu de

[1737] Alors que certains étaient dotés de règles de conflits d'origine légale (pour un exposé des différentes lois étrangères disposant d'une règle de conflit (v. Gérard LEGIER, « Le règlement " Rome II " sur la loi applicable aux obligations non contractuelles », art. préc., spéc. n° 34), pour d'autres, au contraire, comme la France, la règle de conflit avait une origine jurisprudentielle.

[1738] L'ensemble de ces solutions ignore totalement la neutralité qui caractérise par principe une règle de conflit (sur ce caractère, v. *supra :* 576).

[1739] La clause d'exception étudiée par la suite ne saurait s'analyser ainsi.

[1740] V. **A.** WEILL, *Un cas épineux de compétence législative en matière de responsabilité délictuelle, op. cit.*, spéc. p. 553 préc. – Yvon. LOUSSOUARN, Pierre BOUREL et Pascal DE VAREILLES-SOMMIERES, *Droit international privé, Dalloz*, 9e éd., 2007, n° 401-1, p. 549. – Pierre MAYER et Vincent HEUZE, *Droit international privé*, 9e éd, *op. cit.*, n° 685, p. 517.

[1741] « *le dommage révèle cette rupture que le droit de la responsabilité cherche à effacer ou atténuer* » (**A.** WEILL, *Un cas épineux de compétence législative en matière de responsabilité délictuelle, op. cit.*, spéc. pp. 552 et 554).

réception qui coïncide lui-même fréquemment de la résidence du « spammé ». Toutefois, le lieu de la réception des *e-mails* apparaît de plus en plus fortuit, les progrès technologiques permettent désormais d'être presqu'en permanence connecté au réseau et donc de pouvoir consulter et recevoir ses messages en tout lieu. Pour surmonter ces difficultés, il serait intéressant de proposer comme critère de rattachement le lieu de résidence habituelle du « spammé » qui a le mérite de la stabilité. Cette proposition, nous le verrons, sera d'autant plus pertinente que ce critère sera également proposé en matière d'atteinte aux droits de la personnalité [1742] et répondra ainsi à un souci de cohérence dans le cas où le *spamming* constituerait à la fois un dommage et une atteinte aux droits de la personnalité [1743].

2. Un rattachement dérogatoire exceptionnel : la clause d'exception

574. Une exception fondée sur des liens parfois plus étroits. En cas de règles de conflit trop rigides, leur mise en œuvre risque de conduire à appliquer une loi qui n'aurait que des liens très ténus avec la situation à régir. Afin d'éviter cet inconvénient, le règlement a prévu une clause d'exception qui autorise à « *écarter la loi normalement applicable pour appliquer une loi qui a des liens plus étroits avec le rapport juridique en cause* » [1744]. En vertu de cette clause, s'« *il résulte de l'ensemble des circonstances que le fait dommageable présente des liens manifestement plus étroits avec un pays autre* » que celui du lieu du dommage ou de la résidence commune habituelle des parties [1745], la loi de ce pays évincera la loi désignée en principe par le règlement. Cette prise en compte de la notion de proximité [1746] consacre ainsi le concept de « *centre de gravité du délit* » [1747], point de concentration des rattachements. La clause d'exception tend ainsi à se rapprocher de la « *proper law of the tort* » existant en droit américain [1748] tout en conservant sa spécificité puisqu'elle demeure

[1742] V. *infra :* n° 582.

[1743] Il en est sera ainsi par exemple dans le cas où un « spammé » victime d'une attaque de *mail bombing*. D'une part, la victime pourra agir pour l'atteinte portée à la protection de ses données nominatives en raison de leur collecte illicite par le « spammeur ». D'autre part, il non seulement pour l'atteinte à son droit à sa tranquillité en raison de la réception massive d'*e-mails*, mais pourra également agir en responsabilité délictuelle pour le dommage subi (perte d'*e-mails* légitimes, par exemple).

[1744] Hélène GAUDEMET-TALLON, *Le pluralisme en droit international privé : Richesses et faiblesses*, recueil préc., spéc. n^{os} 359 et s., p. 328 et s. – Pour une application en matière de délit, *ibid.*, préc., spéc. p. 331 s., n° 338 s.

[1745] Art. 4.3 du règl. (CE) n° 864/2007 préc.

[1746] Paul LAGARDE, *Le principe de proximité dans le droit international privé contemporain*, *RCADI* 1986, tome 196 (ce principe exprime, en matière de conflits de lois, « *l'idée du rattachement d'un rapport de droit à l'ordre juridique avec lequel il présente les liens les plus étroits* », *id.*, spéc. pp. 9-25).

[1747] Bernard AUDIT, *Droit international privé, op. cit.*, spéc. n° 799, p. 664.

[1748] Cette théorie a été dégagée par J HC MORRIS, *The proper Law of a tort, Harward Law Review*, 1951, vol. 64, p. 881 et s. – Au milieu du XX^{e} siècle, émerge aux États-Unis un courant de pensée pionnier, né en réaction à la jurisprudence de la Cour Suprême jugée trop conservatrice qui se pose en censeur des solutions jurisprudentielles traditionnelles. Ce mouvement, dit « réaliste », prône un raisonnement pragmatique en matière de conflits de lois. Cette approche plus souple des situations de conflits de lois exhorte les juges à prêter une attention toute

une exception stricte. Cette théorie invite à se détacher d'une application mécanique et aveugle de la *lex loci delicti* conduisant à retenir le lieu du délit comme élément de rattachement exclusif dans la détermination de la loi compétente, pour s'interroger sur les éléments qui pourraient entretenir un lien plus étroit avec le délit. Le lieu du délit apparaît parfois comme très accessoire par rapport aux intérêts en cause. Il en est ainsi tout particulièrement lorsque le délit s'est produit de manière fortuite. Dans cette hypothèse, il serait dès lors judicieux de rechercher la loi la plus appropriée (la « *proper law* ») au cas d'espèce, au regard d'éléments qui présenteraient un lien manifeste avec le rapport juridique (lieu du délit, nationalité et domicile des parties). Cette méthode ne consiste pas en une simple évaluation mathématique basée sur le résultat obtenu de l'addition des divers points de contact mais procède d'une appréciation qualitative de ces derniers au regard des circonstances de l'espèce. Cette analyse aboutirait ainsi à une solution considérée comme la plus adaptée à la situation en cause [1749]. La conception américaine apparaît donc plus souple que celle adoptée de ce côté-ci de l'Atlantique.

575. Conditions d'application. L'article 4.3 du règlement Rome II a encadré les conditions d'admissibilité de cet assouplissement : « [s']*il résulte de l'ensemble des circonstances que le fait dommageable présente des liens plus étroits avec un pays autre que celui* [où le dommage survient] *ou* [celui de la résidence commune de la personne poursuivie et de la victime], *la loi de cet autre pays s'applique* ». De façon pragmatique, l'article 4.3 précise cette disposition en s'appuyant d'une illustration concrète : « *Un lien manifestement plus étroit avec un autre pays pourrait se fonder, notamment, sur une relation préexistante entre les parties, telle qu'un contrat présentant un lien étroit avec le fait dommageable en question* ». Le recours au terme « *manifestement* » impose une existence évidente de liens

particulière aux préoccupations sociales en écartant tout attachement inconditionnel et artificiel aux règles de droit auquel conduit une application stricte de la lettre des textes. Ainsi, sont-ils invités à rejeter toute réflexion juridique guidée spontanément par des réflexes mécaniques, systématiques pour faire évoluer le droit vers une approche plus « socialisante », transformant ainsi le juge en un artisan social capable de façonner et de rendre des décisions à hauteur des attentes de la société. Ce courant a progressivement pénétré les règles de conflits de lois en matière extracontractuelle. Son influence croissante a conduit à une prise de conscience en la matière qui s'est traduite par une critique de plus en plus acerbe des solutions imprégnées du dogme de la territorialité au profit de règles de rattachement plus pragmatiques et donc davantage en cohérence avec la réalité sociale environnante (sur cette « révolution » américaine, v. HANOTIAU, *Le droit international américain*, L.G.D.J., 1979, n^os^ 68-85 et 111-176 et n^os^ 259 s. – David F. CAVERS, " A Critique of the Choice-of-Law Process ", 47 *Harv. L. Rev.* 173 (1933). – Brainerd CURRIE, " Notes on Methods and Objectives in the Conflict of Law ", 1959 *Duke L. J.* 171 (1959).

[1749] Sur cette théorie, v. Pierre BOUREL, *Les conflits de lois en matière d'obligations extra-contractuelle, op. cit.*, p. 41 et s.

étroits entre un pays et la situation en cause, et révèle que ce correctif a vocation à s'appliquer de façon exceptionnelle [1750].

576. Évaluation critique de la clause d'exception. La clause d'exception apporte la flexibilité souhaitée par la référence à la proximité. Par ailleurs, l'adoption de cette clause permet de préserver la finalité première de la règle de conflit, à savoir la désignation de « la loi la plus concernée » et la plus « à même » de trancher le litige. Cette solution garantit également le caractère, en principe, neutre de la règle de conflit en ce sens que la clause d'exception n'a pas vocation à s'attacher au contenu matériel des droits nationaux en concurrence. Selon le professeur Paul LAGARDE, ce principe « *est simplement une grille de lecture pour interpréter un certain nombre de règles de conflits, mais qui n'a rien d'explicite. Elle s'inspire de l'idée qu'il ne faut pas laisser un État régir des situations sur lesquelles il ne doit normalement pas avoir prise parce qu'elles sont trop éloignées de lui* » [1751]. Cette méthode, dont on peut saluer la souplesse, suscite néanmoins la critique eu égard au large pouvoir d'appréciation conféré au juge dans la détermination de la loi compétente. Cette latitude laissée au juge rend alors les décisions incertaines et les exposent à un risque accru de contestations [1752]. Or, l'objectif de la règle de conflit est précisément d'offrir au juge une certaine sécurité intellectuelle en désignant l'application d'une loi précise ou facile à identifier. Ce sont ces mêmes craintes qui ont conduit le professeur Paul LAGARDE à considérer le développement du principe de proximité comme une « *formidable régression* » [1753] dans la résolution des conflits de lois. Enfin, dans la mesure où cette méthode s'appuie sur un faisceau d'indices résultant de l'environnement du délit (nationalité, immatriculation des véhicules)…, la désignation de la loi la plus appropriée est susceptible de conduire à désigner la loi d'un État sur lequel aucun des éléments constitutifs du délit complexe ne s'est produit. Tel serait le cas par exemple de l'envoi par un « spammeur » de messages vers des destinataires localisés dans un État donné, mais ressortissants d'un autre

[1750] Sur cette nécessité d'une application « *véritablement exceptionnelle* » de cette clause, v. Bernard AUDIT *Droit international privé, op. cit.*,spéc. n° 107, p. 89 (expliquant qu'elle « *porte atteinte à la prévisibilité que procure normalement* [*la règle de conflit*] »). – V. ég. Wilhem WENGLER énonce que : « *les justiciables ont plus intérêt à connaître avec certitude le droit applicable ultérieurement dans un État du for qu'à savoir que le juge est prêt à appliquer le droit qui selon lui est déterminé par la somme la plus importante des éléments de rattachement. Je vais même jusqu'à considérer que la clause échappatoire constitue une violation de ce droit fondamental qu'est le droit à la certitude du droit* » (« L'évolution moderne du droit international privé et la prévisibilité du droit applicable », *Rev. crit. DIP* 1990, p. 657 et s., spéc. p. 668). – V. ég. *infra* : n° 576.

[1751] Paul LAGARDE, *Le principe de proximité dans le droit international privé contemporain,* recueil préc., spéc. p. 29 s.

[1752] P. MAYER exprime parfaitement cette idée : « *La méthode du groupement des points de contact fait perdre en prévisibilité ce qu'elle fait gagner en souplesse* » (Pierre MAYER et Vincent HEUZE**,** *Droit international privé, op. cit.*, spéc. n° 679, p. xx). – V. Paul LAGARDE qui, tout en reconnaissant sa souplesse manifeste, reconnaît sa grande imprévisibilité (Le principe de proximité dans le droit international privé contemporain, recueil préc., *loc. cit.*).

[1753] Paul LAGARDE, *Le principe de proximité dans le droit international privé contemporain,* recueil préc., spéc. p. 45.

État. Si les juges estiment que la loi la plus appropriée est la loi de la nationalité des destinataires, cette dernière sera désignée compétente alors même que ni l'envoi (fait générateur du *spamming*) ni la réception du message (dommage causé par le *spamming*) ne sont localisés sur ce territoire. L'ensemble de ces remarques conduit ainsi à plaider pour un recours exceptionnel à la notion de proximité d'autant que la mise en œuvre de ce correctif apparaît délicate en pratique et la question se pose de savoir comment le manier [1754].

577. Bilan. À l'issue de cette analyse, il convient de reconnaître que le règlement Rome II est venu mettre fin aux incertitudes existantes en droit français dans les cas de délits complexes en se prononçant clairement en faveur de la loi du lieu du dommage. Malgré cet effort d'harmonisation, son champ d'application ne couvre pas toutes les matières, certaines apparaissant comme « *les mal* aimé[e]s *du règlement Rome II* » [1755]. En particulier, la question de la loi applicable aux obligations délictuelles découlant d'atteintes à la vie privée et aux droits de la personnalité est expressément exclue de son champ d'application par l'article 1-2 g), faute de consensus trouvé sur cette problématique.

§ 2. LA LOI APPLICABLE EN MATIERE D'ATTEINTES AUX DROITS DE LA PERSONNALITE DES « SPAMMES »

578. L'atteinte qui peut être portée aux droits de la personnalité des « spammés conduit à s'interroger sur la règle de conflit qui a vocation à s'appliquer. Cette matière a fait l'objet de nombreux débats au niveau européen pour tenter de trouver une règle de conflit uniforme [1756]. À défaut d'accord entre les États membres, ces derniers doivent donc revenir à leurs règles de conflit nationales afin de déterminer l'élément de rattachement et par

[1754] À cet égard, Andreas BUCHER énonce clairement cette problématique : « *la proximité est un critère qui permet à la jurisprudence de disposer d'une certaine flexibilité, de s'écarter d'une règle de conflit qui paraît rigide. Mais ce critère* […] *ne précise pas de quelle manière il convient de procéder* » (« Vers l'adoption de la méthode des intérêts ? Réflexions à la lumière des codifications récentes » *in Droit international privé, Travaux du comité fr de DIP* 1993-1194, 1994-1995, éd. A. PÉDONE, coll. *Droit international privé*, 1996, p. 209 et s.). – Le professeur Horatia MUIR WATT suggère de s'en remettre aux principes généraux, soulignant que « *le droit international privé a toujours entretenu des relations privilégiées, intimes avec les principes généraux* […]. *Loin de surprendre, la présence des principes généraux est en quelque sorte congénitale au droit international privé* » (« Les principes généraux en droit international privé français », *JDI* 1997, p. 403 et s., spéc. p. 404). Elle précise à ce titre qu'« *il pourrait être utile, au vu des caractéristiques contemporaines des règles conventionnelles de conflit, de reconnaitre l'existence de principes généraux régissant la mise en œuvre des clauses d'exception ou la concrétisation du rattachement par " les liens les plus étroits " (le type de paramètre utilisé ; le seuil de la proximité, etc.)* » (*id.*, spéc. p. 410) afin de mieux saisir les mécanismes qui président à « *la mise en œuvre des clauses d'exception ou la concrétisation du rattachement par " les liens les plus étroits "* » (*id.*, spéc. *loc. cit.*), en fournissant des critères directifs auxquels les juges pourraient se référer tels que, par exemple, « *le type de paramètre utilisé ; le seuil de la proximité, etc.* » *id.*, spéc. *loc. cit.*).

[1755] Louis PERREAU-SAUSSINE, « Les mal-aimés du règlement Rome II : les délits commis par voie de média », art. préc.

[1756] Sur ce point, v. Gérard LEGIER, « Le règlement " Rome II " sur la loi applicable aux obligations non contractuelles », art. préc., spéc. n[os] 16 et 17.

conséquent, la loi applicable (A.). Toutefois, nous verrons que l'application de la règle de conflit française ne permet pas d'aboutir à une solution pleinement satisfaisant en matière de *spamming*. Ce constat nous conduira dès lors à proposer un nouveau critère de rattachement (B.).

A. LA MISE EN ŒUVRE DE LA REGLE DE CONFLIT FRANÇAISE

579. L'article 3 du Code civil. En droit international privé français, la règle de conflit applicable aux atteintes aux droits de la personnalité a été à l'origine dégagée de l'article 3 alinéa 1er du Code civil qui désignait par principe la loi du lieu du délit dans le cadre d'un conflit national [1757]. Cette règle a été par la suite internationalisée par la Cour de cassation dans le célèbre arrêt *Lautour* : « *Attendu qu'en droit international privé, la loi territoriale compétente pour régir la responsabilité civile extra-contractuelle* […] *est la loi du lieu où le délit a été commis* » [1758]. Puis, la jurisprudence a entendu maintenir ce principe et ce, indépendamment de la nationalité des parties [1759]. La Cour de cassation a adopté à la suite de cet arrêt une position très ferme quant à la détermination de la loi applicable : « *sauf conventions contraires, les obligations extra-contractuelles sont régies par la loi du lieu où est survenu le fait* [dommageable] *qui lui a donné naissance* » [1760].

580. La problématique des délits complexes. Malgré un principe qui semblait inébranlable, cette solution ne pouvait perdurer en raison des évolutions que connurent les comportements délictueux. En effet, l'arrêt *Lautour* avait été rendu dans le contexte d'un délit simple (accident de la circulation où le fait générateur et le dommage sont survenus sur le territoire d'un même État), à une époque où les délits complexes étaient encore considérés comme un phénomène rare. Toutefois, la tendance s'est rapidement inversée [1761], la

[1757] « *Les lois de police et de sûreté obligent tous ceux qui habitent le territoire* » (art. 3 al. 1er C. civil).
[1758] Cass. civ. 25 mai 1948, *Lautour*, *JCP* 1948, G., II. 4542, note M. Vasseur ; *D.* 1948, p. 357, note P. L. ; *Rev. crit. DIP* 1949, p. 89, note H. BATIFFOL ; *GAJFDIP*, 5e éd., *Dalloz*, 2006, n° 19, p. 164 et s., *S.* 1949. 1. 21, note Niboyet. – V. ég. André LUCAS, Jean DEVEZE, Jean FRAYSSINET, « *en droit français, la réparation de l'ensemble des dommages susceptibles d'être causés par la voie des réseaux numériques relèvera de la lex loci delicti* » (*Droit de l'informatique et de l'Internet, op. cit.*, spéc. n° 715, p. 470).
[1759] Cass. civ. 1re, 30 mai 1967, *Kieger c/ Amigues, Rev. crit. DIP* oct.-déc. 1967, p. 728, note P. Bourel ; *JDI* 1967, p. 622 et s., note B. G. *; D.* 1967, jurispr., p. 629 et s., note P. Malaurie ; *JCP* 1968, éd. G., II. 15456, note A. Jack Mayer (« *Quelle que soit la nationalité des parties, la loi compétente pour régir la responsabilité extra-contractuelle est la loi du lieu où le fait dommageable s'est produit* »).
[1760] Cass. civ. 1re, 1er juin 1976, *Luccantoni, JDI* 1977, p. 91, note B. Audit ; *D.* 1977, jurispr., p. 257 et s., note F. Monégier ; *JCP* 1979. éd. G., II. 19082, note F. Chabas (en l'espèce, a été « *cassé le jugement, qui statuant sur une demande intentée devant un tribunal français, en réparation de dommages causés par une collision d'automobiles survenue en Espagne, a écarté l'application de la loi espagnole revendiquée par le défendeur et appliqué la loi française* »).
[1761] v. *supra : la multiplication des délits complexes* : n° 518.

multiplication de ce type de délit conduisant la jurisprudence à devoir reconsidérer sa position. En effet, la solution traditionnelle ne permettait pas de déterminer dans les cas où le lieu du fait générateur et celui du dommage étaient distincts, si « le lieu du délit » devait s'entendre comme celui du fait générateur ou comme celui du dommage. Face à cette incertitude, la question de la dissociation géographique des éléments constitutifs du délit a donné lieu à des solutions jurisprudentielles successives extrêmement diverses empêchant ainsi d'aboutir à une solution unique définitive. Après s'être prononcée tout d'abord en faveur de la loi du « *lieu où le dommage a été réalisé* » [1762], la Cour de cassation s'est orientée, à partir de 1997, vers un système alternatif, en jugeant que le lieu où le fait dommageable s'est produit « *s'entend aussi bien de celui du fait générateur que du lieu de réalisation de ce dernier* » [1763]. À cet égard, le professeur Hélène GAUDEMET-TALLON, soulignant les difficultés de trancher catégoriquement en faveur de l'un ou l'autre de ces rattachements, a considéré qu'« *il est impossible de choisir l'un des deux critères de rattachement et de n'accorder aucune place à l'autre* » [1764]. Des arrêts ultérieurs ont recherché la loi qui entretenait « *les liens les plus étroits avec le fait dommageable* » [1765], pour ensuite se tourner vers la loi du lieu du fait générateur [1766].

581. L'exemple du *spamming*. L'absence de jurisprudence stable permettant de déterminer la loi applicable en cas d'atteinte aux droits de la personnalité peut ainsi conduire à désigner soit la loi du lieu du fait générateur soit celle du lieu du dommage. Or, l'une et l'autre révèlent en pratique leurs limites. D'une part, techniquement, retenir comme critère

[1762] Cass. civ. 1re, 8 févr. 1983, *Horn y Prado*, *JDI* 1984, p. 123 et s., note G. Légier (« *en droit international privé français* […] *la loi territoriale compétente pour gouverner la responsabilité civile est la loi du lieu où le dommage a été réalisé* ». Toutefois en l'espèce, l'acte générateur et le dommage étaient survenus en France).

[1763] Cass. Civ. 1re, 14 janv. 1997, *Sté Gordon & Breach Science Publishers*, *Rev. crit. DIP* 1997, p. 504, note J.-M. Bischoff ; *D.* 1997, p. 177 et s., note M. Santa-Croce ; *JCP* 1997, éd. G., II. 22903, note H. Muir Watt).

[1764] Hélène GAUDEMET-TALLON, *Le pluralisme en droit international privé : richesses et faiblesses*, recueil préc., spéc. n° 211, p. 222.

[1765] Cass. civ. 1re, 11 mai 1999, *Mobil North Sea*, *JCP* 1999, éd. G., II. 10183, note H. Muir Watt ; *D.* 1999, somm., pp. 295-296, obs. B. Audit ; *Rev. crit. DIP* avr.-juin 2000, p. 199 et s., note J.-M. Bischoff ; *JDI* 1999, p. 1048 et s., note G. Légier (en l'espèce, la cour d'appel qui avait recherché, en raison de la multiplicité des lieux de commission du fait générateur du dommage, le pays qui présentait les liens les plus étroits avec le fait dommageable et avait considéré que « *la localisation en dehors* [du pays où s'est produit le dommage] *de certains éléments du fait générateur n'était pas déterminante* [et avait] *exactement déduit que la loi applicable était* […] *celle du lieu où s'était produit le dommage* »). – Et dernièrement, v. Cass. civ. 1re, 27 mars 2007, 1re ch., *Bureau Veritas*, pourvoi n° 05-10.480 ; *Juris-Data* n° 2007-038216 ; *Resp. civ. assur.* juin 2007, comm. 194, p. 22 et s. ; *D.* 2007, actu., p. 1074 et s., obs. I. Gallmeister ; *Rev. crit. DIP* avr.-juin 2007, p. 405 et s. ; note D. Bureau ; *JDI* 2007, p. 949, note G. Légier (« *la loi applicable à la responsabilité extra-contractuelle est celle de l'État du lieu où du fait dommageable s'est produit, ce lieu s'entendant en cas de délit complexe aussi de celui du fait générateur du dommage que du lieu de réalisation de ce dernier* »).

[1766] Cass. civ 1re, 23 janv. 2007, *Caisse d'épargne De Sarrebruck*, *Rev. crit. DIP* oct.-déc. 2007, p. 760 et s., note O. Boskovic ; *D.* 2007, études, p. 1244 et s., note N. Bouche (à propos d'un délit bancaire, la Cour de cassation avait toutefois retenu que le fait générateur et le dommage s'étaient réalisés dans le même pays, pour une critique de cet arrêt, v. not. Olivera BOSKOVIC, note préc.) ; 30 janv. 2007, *M. Lamore c/ Universal Studios Inc. et autres*, *Rev. crit. DIP* oct.-déc. 2007, p. 769, note T. Azzi (« *attendu que* […] l*a législation du pays où la protection est réclamée* [en l'espèce, protection des droits d'auteur], *n'est pas celle du pays où le dommage est subi* [la France] *mais celle de l'État sur le territoire duquel se sont produits les agissements délictueux* [les États-Unis], *l'obligation de réparation n'étant que la conséquence éventuelle de ceux-ci* »).

de rattachement le lieu d'envoi des *spams* peut engendrer des situations de blocage. L'expérience démontre en effet que les « spammeurs » ont tendance à recourir à divers stratagèmes techniques pour masquer l'origine de leurs envois (« PC zombies », *proxys*, …) [1767]. La multiplicité des faits générateurs réels, voire erronés, qui résulte de cette situation complexifie leur localisation jusqu'à parfois même la rendre impossible [1768]. Juridiquement, la loi du lieu du fait générateur apparaît inadéquate en raison des profondes divergences existantes entre les législations, non seulement celles relatives à la protection des données à caractère personnel mais aussi celles régissant spécifiquement le *spamming* [1769]. Cette solution inciterait en effet le « spammeur » à s'établir volontairement sur le territoire d'un État où la législation est la moins sévère et aboutirait ainsi à laisser impuni un grand nombre de « spammeurs » au détriment des victimes. Cette solution n'apparaît donc pas viable. D'autre part, même si la loi du lieu du dommage (lieu de réception du message) permettait de faire le contrepoids des critiques précédemment formulées en permettant d'échapper au risque de fraude aux droits des victimes, sa mise en œuvre demeure problématique, notamment à cause des cas de plus en plus fréquents où le lieu du dommage est fortuit. L'ensemble de ces inconvénients conduit ainsi à rechercher un nouveau critère stable de rattachement qui permettrait de pallier ces difficultés.

B. LA RECHERCHE D'UN NOUVEAU CRITERE STABLE DE RATTACHEMENT

582. Proposition : la résidence habituelle du « spammé ». Les obstacles inhérents à la localisation du fait générateur et à celle du dommage conduisent à proposer un nouveau critère de rattachement en matière d'atteinte aux droits de la personnalité. Celui-ci consisterait à rejoindre la proposition suggérée en matière de compétence juridictionnelle en localisant fictivement le préjudice au lieu de la résidence habituelle du « spammé » [1770]. Cette solution avait déjà été proposée à plusieurs reprises en doctrine et devrait retrouver une certaine actualité [1771] dans la mesure où elle répond à un souci de pragmatisme. Comme le souligne le professeur Hélène GAUDEMET-TALLON, « *ce domicile, peut en effet, être*

[1767] Sur ces techniques d'envoi, v. *supra* : n° 95 et s.
[1768] Philippe MALAURIE soulignait que « *la lex loci delicti est sans doute une règle de conflit qui n'st guère satisfaisante, car elle s'attache à des leiux fortuits, qui par hypothèse, sont accidentels* » (note sous Cass. civ. 1re, 30 mai 1967, *Kieger*, arrêt préc., *D.* 1967, jurispr., p. 629 et s., spéc. p. 630).
[1769] V. *supra :* titre 2, Partie 1 : « Des législations spéciales fragiles ».
[1770] V. *supra :* n° 558.
[1771] V. en ce sens, Catherine KESSEDJIAN, « Rapport de synthèse » *in* Katharina BOELE-WOELKI et Catherine KESSEDJIAN, *Internet, Which Court Decides ? Which Law Applies ?, op. cit.*, spéc. p.152. — Pour une solution identique en cas d'atteinte aux droits de propriété intellectuelle sur l'internet, v. par ex. François DESSEMONTET, « Internet, la propriété intellectuelle et le droit international privé », art. préc., spéc. p. 57.

considéré comme " localisant " mieux le rapport juridique » [1772] puisque c'est à « *l'endroit où vit habituellement* [la victime] *que sera ressentie le plus fortement par elle l'atteinte à ses droits ; c'est là qu'elle subira le préjudice dont elle demande réparation* » [1773]. Dans cette veine, le Groupe Européen de Droit International Privé (GEDIP) [1774] a prévu une présomption selon laquelle l'obligation non contractuelle a les liens les plus étroits « *en cas d'atteinte à la vie privée ou aux droits de la personnalité, ou de diffamation, avec le pays dans lequel le dommage est survenu ou menace de survenir ; le dommage est présumé survenir dans le pays où la personne lésée a sa résidence habituelle au moment du fait dommageable* » [1775]. Par ailleurs, l'article 7 de l'avant-projet de proposition de règlement du Conseil sur la loi applicable aux obligations non contractuelles, dit « projet Rome II », établi par la Commission européenne, soumettait également l'ensemble de la question (atteinte à la vie privée ou aux droits de la personnalité ou diffamation) à la loi du « *pays où la personne lésée a sa résidence habituelle au moment de la survenance du délit* » [1776]. Cette solution apparaît pertinente en ce sens que les droits de la personnalité entretiennent, comme leur nom l'indique, une relation « charnelle », quasi « épidermique » avec leur titulaire. En raison de leur proximité, voire de leur fusion avec cette personne, ces droits ne peuvent être détachés géographiquement de la localisation de cette dernière. Cette solution présente l'avantage de la prévisibilité. De surcroît, il convient de souligner que si la CJCE reste pour le moment hostile à toute proposition qui consisterait à retenir la compétence de la loi du lieu de résidence habituelle de la victime, il ne faut pas oublier que cette position concerne

[1772] Hélène GAUDEMET-TALLON, *Le pluralisme en droit international privé : Richesses et faiblesses*, recueil préc., spéc. n° 213, p. 224. – V. ég. Pierre BOUREL, *Du rattachement de quelques délits spéciaux en droit international privé français*, *RCADI* 1989, tome 214, p. 253 et s, spéc. pp. 338-339 (« *Il s'agit là d'une localisation à la fois juridique et sociologique. Localisation juridique, car elle prend en considération la nature spécifique du délit. S'agissant d'atteintes à la personne humaine, le siège de la personnalité, c'est-à-dire le domicile, constitue un facteur déterminant. Localisation sociologique, car si les droits protégés ont, en tant qu'attributs de la personne, une signification individuelle, ils possèdent également une signification sociale ou relationnelle.* […] *Or, le domicile (ou la résidence habituelle) est par excellence le lieu qui exprime le siège de cette attitude, de cette relation* » (*id*., spéc. p. 338).

[1773] Pierre BOUREL, *Du rattachement de quelques délits spéciaux en droit international privé français*, recueil préc., spéc. p. 338 (précisant toutefois que la loi du domicile qu'il propose « *n'est pas* […] *un succédané de la lex loci delicti commissi* ». […] « *La loi du domicile de la victime n'est ni une loi personnelle ni la loi du lieu, réel ou fictif, de commission du fait dommageable. Elle est l'expression directe du principe de proximité, dont la mise en œuvre demeure indifférente sinon à toute qualification du rapport juridique, du moins au classement de celui-ci dans une catégorie préétablie du droit international privé* [statut personnel ou statut délictuel] (*id.*, spéc. p. 339).

[1774] Créée en 1991, cette association de droit luxembourgeois, composée d'experts, membres des Universités des États membres de l'Union européenne ou d'organisations internationales, s'intéresse aux interactions du droit international privé et du droit européen. Elle vise à constituer un lieu d'échanges d'informations et d'idées grâce aux comptes rendus des réunions de travail qu'elle élabore, aux conclusions auxquels certains travaux peuvent aboutir et a pour mission la diffusion d'informations de portée générale à des fins scientifique ou académique. – Pour plus d'informations sur sa composition, son rôle, consulter le site du GEDIP, disponible sur : http://www.gedip-egpil.eu.

[1775] Article 4 a de la proposition pour une convention européenne sur la loi applicable aux obligations non contractuelles, texte adopté lors de la réunion de Luxembourg des 25-27 septembre 1998, *Rev. crit. DIP* 1998, p. 802.

[1776] Cyril NOURRISSAT et Édouard TREPPOZ, « Quelques observations sur l'avant-projet de proposition de règlement du Conseil sur la loi applicable aux obligations non contractuelles " Rome II " », *JDI* 2003, spéc. p. 7 et s., n° 33, p. 29.

exclusivement la matière juridictionnelle [1777]. Il convient également d'ajouter que s'il existe une certaine réticence envers le tribunal du demandeur (*forum actoris*) en matière de compétence juridictionnelle, se justifiant notamment par la crainte de compromettre les intérêts du défendeur, cet argument ne saurait prospérer en matière de conflits de lois puisque l'objectif est, dans ce cas, de désigner la loi qui présente, de façon objective, les liens les plus étroits avec la situation en cause [1778].

*

* * *

583. Grâce à l'adoption du règlement Rome II, l'effort d'harmonisation des règles de droit international privé en matière d'obligations extracontractuelles à l'échelle communautaire est désormais achevé. En retenant la compétente la loi du lieu du dommage, ce règlement offre les moyens de désigner objectivement une loi unique applicable aux obligations délictuelles au sein des États de l'Union européenne. Elle garantit également une plus grande prévisibilité des solutions et « *rend sans intérêt le forum shopping et contribue à la réalisation de l'espace européen de la justice* » [1779]. La pertinence de cette solution se vérifie également en matière de *spamming* étant donné les divergences de systèmes juridiques. Toutefois, cet effort pourrait être vain dès lors qu'en matière d'atteinte aux droits de la personnalité, les règles de conflits traditionnelles peuvent aboutir à l'application de la loi du lieu du fait générateur ou à celle du lieu du dommage. Ce risque se manifeste tout particulièrement dans le cas du *spamming* lorsque celui-ci constitue à la fois une atteinte aux droits de la personnalité et un dommage. Ce cas de figure pourrait alors être régi par deux règles de conflit selon le type d'atteinte en cause, ce qui aurait pour effet d'aboutir à la désignation de deux lois internes distinctes. Cette conséquence nous a conduits à proposer, en matière délictuelle comme en matière d'atteintes aux droits de la personnalité, un critère de rattachement unique qui se caractérise non seulement par sa facilité d'identification mais également par sa prévisibilité, à savoir : le lieu de résidence du « spammé ».

[1777] La décision rendue par la CJCE dans l'affaire *Marinari* était notamment fondée sur la volonté de ne pas s'éloigner de manière démesurée de la règle de compétence générale fixée par l'article 2 de la Convention du 27 septembre 1968, et reprise par le règlement Bruxelles I, qui fixe la compétence de la juridiction du domicile du défendeur. Il en résultait ainsi que l'option de compétence offerte au demandeur ne pouvait pas être étendue au-delà des circonstances particulières qui l'autorisent (sur cet arrêt, v. *supra :* n° 559).
[1778] Sur l'objectif distinct poursuivi par ces deux types de règles de conflit, v. *supra* : 534.
[1779] Gérard LEGIER, « Le règlement " Rome II " sur la loi applicable aux obligations extracontractuelles », art. préc., spéc. n° 30.

CONCLUSION DU CHAPITRE 2

584. Cette étude a permis de mettre en évidence que les solutions issues de l'application des règles de conflit offertes par le droit international privé se révèlent insuffisantes, tant en matière de compétence juridictionnelle que législative, pour résoudre l'ensemble des hypothèses de *spamming*.

585. S'agissant de la désignation de la juridiction compétente, le règlement Bruxelles I ne parvient pas résoudre les difficultés que posent les hypothèses les plus complexes de *spamming* où le lieu du fait générateur et celui du dommage ne sont plus concentrés sur un seul territoire. Nous avons pu en effet constater que le règlement n'offre aucune réponse en cas de multiplicité des faits générateurs, hypothèse pourtant courante en matière de *spamming* [1780]. De même, la règle de conflit conduisant à désigner compétente la juridiction du lieu du dommage ne semble guère pertinente en raison de la multiplication des lieux de réception des *e-mails*. Les conclusions sont identiques lorsque le « spammeur » est établi hors de l'Union européenne. Dans ces circonstances, il est apparu intéressant de suggérer la création d'un nouveau critère de rattachement spécifique au *spamming*, à savoir : le lieu de résidence habituelle du « spammé ». Répondant à un souci de pragmatisme, cette solution permettrait de surmonter les difficultés tenant notamment à l'identification du lieu du dommage lorsque ce dernier est fortuit, une hypothèse devenue désormais fréquente. Par ailleurs, la permanence qui caractérise la résidence permettrait d'assurer la sécurité juridique en permettant de connaître, de façon prévisible, la juridiction compétente.

586. En matière de compétence législative, la mise en œuvre du règlement Rome II en matière de *spamming* n'aboutit pas non plus à des solutions pleinement satisfaisantes, en particulier lorsque cette pratique porte à la fois une atteinte aux droits de la personnalité et engendre un dommage matériel. En appliquant les règles de conflits fixées par le règlement Rome II, cette double atteinte déboucherait sur une situation impraticable dans laquelle le « spammé » pourrait être soumis à des lois différentes. Afin d'assurer la cohérence des solutions applicables à un même litige, il était donc opportun de proposer, en matière de *spamming*, une règle de conflit spécifique pragmatiquement efficace et juridiquement viable. L'examen des différentes situations de *spamming* nous a conduits à retenir, de façon uniforme, la loi du lieu de résidence du « spammé » [1781]. Cette solution serait toutefois

[1780] En raison du recours accru au PC zombies notamment.

[1781] Cette proposition rejoindrait les vœux du professeur Hélène GAUDEMET-TALLON qui, à propos de la structure du droit de la responsabilité, souligne l'importance de privilégier un rattachement unique afin d'assurer

tempérée par l'existence d'une clause d'exception qui serait d'application exceptionnelle dans le cas où une autre loi présenterait des liens plus étroits avec la situation en cause. Ce critère de rattachement unique assurerait ainsi une cohérence globale des solutions en matière de *spamming* dans la mesure où en pratique, la juridiction compétente est plus encline à appliquer ses propres règles de conflit nationales.

la cohérence des solutions. Elle souligne également que si en droit interne, les conditions et les effets de la responsabilité sont clairement distingués, l'importance « *en droit international privé, de toujours maintenir la plus grande unité possible : le fractionnement des questions nées d'un fait délictueux, débouchant sur une pluralité de lois applicables, risque de ruiner la cohésion de la solution juridique donnée ; chaque droit de la responsabilité forme un ensemble cohérent et il me paraît préférable de choisir un système dans son ensemble plutôt que de morceler la situation en utilisant des rattachements divers* » (*Le pluralisme en droit international privé : Richesses et faiblesses*, recueil préc., spéc. p. 226).

CONCLUSION DU TITRE 2

587. Des modifications à apporter en droit international privé. Pour réussir à trouver une solution uniforme et optimale pour traiter les situations de *spamming,* le caractère plurilocalisé de cette pratique imposait une coopération entre États à l'échelle internationale. Toutefois, les initiatives existantes restent limitées quant à leur efficacité et doivent se doubler de réponses juridiques impératives permettant de résoudre les litiges internationaux. À cet égard, l'intervention du droit international privé s'est révélée indispensable pour trancher des litiges présentant un élément d'extranéité et pour lesquels il existe un risque accru de conflits, tant en matière juridictionnelle qu'en matière législative. En confrontant les solutions issues des règles de conflit au cas précis du *spamming*, cette analyse a mis en évidence les incertitudes, voire les incohérences qui peuvent résulter de leur mise en œuvre, non seulement pour la désignation de la juridiction compétente mais aussi de la loi applicable. Ces difficultés nous ont dès lors conduits à explorer une nouvelle voie qui consisterait à proposer une règle de conflit propre au *spamming.* À l'issue de cette recherche, la résidence du « spammé » est apparue comme la solution la plus pertinente et la plus significative, tant en matière juridictionnelle qu'en matière législative. D'un point de vue pratique, ce critère de rattachement apparaît en effet le plus facile à identifier et permettrait en outre de surmonter les difficultés de localisation lorsque le dommage est fortuit. Enfin, cette solution permettrait de faciliter la mise en œuvre de la loi applicable par la juridiction déclarée puisqu'en effet, si en théorie, le principe est l'indépendance des compétences juridictionnelles et législatives, elles restent en pratique intimement liées

588. La question de l'efficacité des jugements étrangers. Outre cette problématique intéressant la création d'un critère de rattachement pertinent, une question demeure, à savoir celle intéressant l'efficacité des jugements français à l'étranger. En effet, corollaire de la compétence internationale des tribunaux nationaux, il convient de s'interroger sur le point de savoir si les décisions peuvent être exécutées dans un pays étranger autre que celui où le litige a été tranché. Plus précisément, il s'agit de déterminer si le « spammé » français et/ou résidant en France qui obtiendrait une décision favorable, pourrait la faire exécuter dans l'État du « spammeur ». En effet, obtenir la condamnation du « spammeur » étranger ne présente d'intérêt que si la décision le condamnant peut être effective dans l'État du « spammeur ». Or, l'État dans lequel la décision est rendue n'a aucune autorité pour l'imposer à un autre pays ; chaque État déterminant unilatéralement les conditions dans lesquelles une décision étrangère peut produire des effets sur son territoire national (sauf convention internationale ou règlement communautaire). Lorsque les *spams*

proviennent d'un État membre, cette question ne pose pas de réelles difficultés dans la mesure où les décisions rendues dans un litige intracommunautaire bénéficient d'une facilité de reconnaissance dans les autres États membres [1782]. En revanche, la question est plus délicate lorsque les *spams* proviennent de pays tiers, ce qui recouvre la majorité des hypothèses. Dans ces circonstances, le « spammé » qui obtiendrait une décision favorable émanant des juridictions françaises, ne disposerait d'aucune assurance que l'État du « spammeur » accepte de mettre à exécution ce jugement [1783]. Voici encore un terrain où la coopération internationale apparaît indispensable, sous peine de rendre ineffective la lutte contre le *spamming*.

[1782] Sur ce point, v. Bernard AUDIT, *Droit international privé, op. cit.*, n^os^ 581 s., p. 478 s.

[1783] Catherine KESSEDJIAN, *La reconnaissance et l'exécution des jugements en droit international privé aux États-Unis*, Economica, Paris, 1987, n^os^ 1 à 158.

589. Cette seconde partie de notre étude nous a permis d'évaluer l'efficacité des solutions offertes par les différents droits sollicités face aux hypothèses retenues comme les plus représentatives de la diversité du *spamming*. Les limites de la protection spéciale nous a en effet conduit à interroger d'autres droits afin de combler les lacunes qui avaient mises en évidence. Il s'agissait d'une part de trouver des fondements répressifs permettant de sanctionner des comportements particulièrement dangereux pour les « spammés » et que la LCEN en particulier a ignorés. À cet égard, le droit pénal de la consommation est apparu comme un fondement intéressant pour punir une forte de *spams* à caractère commercial mais dont le contenu était en outre destiné à tromper les destinataires. Pour sa part, l'escroquerie permet de sanctionner plus largement, tout contenu trompeur, indépendamment de son caractère commercial et qui vise à obtenir la remise de données nominatives ou de somme d'argent. Le recours à ce fondement est particulièrement pertinent dans les hypothèses, devenues désormais fréquentes où le *spamming* et le *phishing* sont des pratiques intimement liées. On ne peut qu'espérer qu'au regard de la multiplication des hypothèses dans lesquelles le *spamming* est le vecteur, ces deux fondements viennent à être davantage invoqués par les « spammés ». Pour l'heure en effet, les seuls cas de *spamming* sanctionnés l'ont été sur le fondement du droit pénal de l'informatique lorsque le *spamming* constitue une infraction autonome. Par ailleurs, les dommages causés par la réception de *spams* imposait d'interroger le droit de la responsabilité civile afin de déterminer s'il pouvait constituer un fondement permettait d'obtenir efficacement la réparation des « spammés ». Il est tout d'abord apparu que seuls les « spammés » ayant subi un dommage particulièrement pourront agir contre le « spammeur » afin d'obtenir une indemnisation de leur préjudice. Face à ce constat, une forte proportion de « spammeurs » échappait ainsi à tout risque de voir leur responsabilité civile engagée et poursuivre ainsi leur activité en toute quiétude. Cette situation était intolérable puisque de nombreux « spammeurs » retiraient d'importants profits au préjudice des « spammés ». Les limites du droit de la responsabilité délictuelle nous a alors conduits à proposer d'une part la reconnaissance en droit français de la faute lucrative afin de prendre en compte de tels comportements et d'autre part, leur sanction par l'introduction de dommages-intérêts inspirés du droit américain. Cette solution reviendrait alors à faire évoluer la fonction du droit de la responsabilité civile initialement indemnitaire vers une fonction répressive. Enfin, une dernière proposition a touché cette fois le droit processuel. En effet, l'impossibilité pour la plupart des « spammés » ne subissant qu'un dommage tout à fait minime, la consécration d'une action de groupe sur le modèle du droit américain est apparu adaptée puisqu'elle permettrait ainsi de regrouper des actions individuelles qui auraient eu

peu de chance de prospérer, sous une action unique permettant alors d'invoquer un dommage suffisamment important pour justifier l'engagement d'une action à l'encontre du « spammeur ».

590. Enfin, malgré les vertus incontestables de notre positif, la recherche d'une protection optimale des « spammés » ne pouvait ignorer le contexte international dans lequel évolue la pratique du *spamming*. Or, les solutions issus de la mise en œuvre de chacun ces droits n'ont pourront avoir d'effets certain que dans les hypothèses où le *spamming* est cantonné au seul cadre « franco-français ». Or, dans la plupart des cas, les situations de *spamming* présentent un élément d'extranéité qui risque d'engendrer des conflits de lois et de juridictions. Dans ces circonstances, à défaut d'instrument juridique international contraignant, emprunter la méthode adoptée en droit international privé s'est révélée indispensable pour trancher ces divers conflits éventuels. Toutefois, la confrontation de cette méthode face au *spamming* a mise en évidence les limites des solutions offertes par les règles de conflit issues du droit international privé positif dans les cas de *spamming* les plus complexes. Ce constat nous a conduits à surmonter cette impasse en recherchant une règle de conflit qui serait pertinente tant en matière législative que juridictionnelle. À l'issue de cette analyse, la résidence habituelle du « spammé » est apparue comme le critère de rattachement le plus pertinent et permettant de surmonter les insuffisances des solutions qui auraient vocation à s'appliquer.

CONCLUSION GÉNÉRALE

591. La question de la rencontre du droit et du *spamming* à travers le prisme de la protection des « spammés » a permis, nous l'espérons, de rendre compte de la diversité de l'objet de notre étude qui en fait toute sa richesse. Si l'essor du *spamming* est relativement récent, son efficacité et son caractère lucratif lui confère, à n'en pas douter, une vocation à perdurer. Cette constatation justifie à elle seule l'intérêt d'avoir consacré notre attention sur le *spamming*. En perpétuelle mutation, ce phénomène poursuit son expansion comme en attestent les nouvelles cibles des « spammeurs » : aux forums de discussion et aux courriers électroniques qui furent les premiers souffre-douleurs des « spammeurs » s'ajoutent dorénavant les téléphones portables, les réseaux sociaux et le réseau *Bluetooth*. Par ailleurs, le *spamming* est apparu comme une pratique polymorphe au regard de la nature des contenus transmis (commerciale, politique, caritative, pornographique) mais aussi des objectifs recherchés. En effet, sa vocation initialement commerciale a progressivement évolué vers des formes plus dangereuses, tant au stade de la collecte des données nominatives qu'à celui de l'envoi des *spams*. S'agissant de la collecte, nous avons pu constater que les « spammeurs » utilisaient des procédés de plus en plus pernicieux pour collecter massivement les données circulant dans les espaces publics de l'internet. S'agissant des envois, des études récentes ont révélé qu'une forte proportion de *spams* était destinée à tromper les destinataires, soit pour les amener à ouvrir des messages contenant des virus et permettant ainsi d'infecter les postes informatiques des victimes, soit pour les conduire à communiquer des données identifiantes en abusant leur confiance (*phishing*). L'agressivité des « spammeurs » s'est également manifestée dans des hypothèses où l'envoi massif de *spams* vers un destinataire unique était clairement destiné à lui nuire. Face à l'ensemble de ces menaces, la recherche d'une protection efficace des « spammés » s'imposait. La technicité du sujet devait nécessairement nous conduire à évaluer l'efficacité d'une protection technique. Cet examen a clairement démontré qu'une réponse exclusivement technique se révélait insuffisante pour traiter la question du *spamming* dans sa globalité. La raison est simple : au-delà des perturbations des systèmes informatiques, le *spamming* met en jeu des droits et libertés, ce qui rend l'intervention du droit inévitable.

592. De manière générale, notre étude a permis de démontrer que le droit n'était pas totalement démuni face à une telle menace technique et qu'il n'était nullement besoin de créer un droit e*x nihilo* comme on a pu le suggérer face à l'avènement de l'internet. Les évolutions législatives actuellement en discussion ont permis de démontrer que notre droit positif est capable de s'adapter pour appréhender des phénomènes techniques nouveaux.

Derrière une innovation technique, il existe des comportements connus qui n'ont pas attendu le développement de l'internet pour se développer. En effet, les nombreuses pratiques qui se multiplient sur la Toile s'inspirent de techniques déjà connues : le *spamming* a pu le démontrer, mais tout comme le *phishing* ou encore l'usurpation d'identité peuvent le confirmer. En revanche, la particularité de ces techniques tient à leur ampleur qui apparaît sans commune mesure par rapport aux phénomènes connus dans le monde réel. L'internet a ainsi joué comme un catalyseur et un amplificateur des phénomènes. Le *spamming* et ses nouvelles formes telles que le *Blue spam* notamment, sont ainsi apparues comme une opportunité d'examiner les questions nouvelles qui se posent en termes de protection des « spammés » et de rechercher si les solutions offertes par les lois existantes étaient adaptées aux menaces identifiées et au besoin de protection exprimé.

593. Au regard du processus du *spamming* et des menaces qui sévissent à différents stades la recherche d'une protection efficace devait être menée sur un double front : d'une part, en matière de protection des données et d'autre part, au niveau des envois. Pour y répondre, nous avons dans un premier temps interrogé les lois spéciales existantes, à savoir : la loi informatique, fichiers et libertés destinée à encadrer l'exploitation des données à caractère personnel et la loi pour la confiance dans l'économie numérique régissant notamment les envois commerciaux et qui prohibent la pratique du *spamming*. La mise en œuvre de ces lois dans le cadre du *spamming* a permis de constater que ces lois ne permettaient pas d'assurer une protection pleinement satisfaisante et efficace des « spammés ». S'agissant tout d'abord de la législation protectrice des données, la confrontation de cette législation au *spamming* a permis de mettre en exergue les limites de cette loi, tant dans sa fonction curative que préventive, comme en témoignent les sanctions peu dissuasives prononcées dans les rares décisions recensées. La législation anti-*spam* a également révélé ses limites dans l'appréhension du *spamming* puisqu'elle ne permet ni de prendre en compte l'ensemble des cas de *spamming* ni d'offrir une protection à l'ensemble des « spammés ». Au-delà de cette analyse, la dimension internationale du *spamming* imposait de déterminer le niveau de protection existant aux delà de nos frontières. La comparaison du droit français et du droit américain a été particulièrement instructive. Les divergences qui existent entre ces deux systèmes juridiques ont permis de mesurer les difficultés qui risquaient de se poser lorsqu'un litige survient dans un contexte international. En particulier, ces divergences risquent de compromettre l'efficacité des solutions issues du droit interne puisque celui s'expose à la concurrence d'autres étrangers qui seront susceptibles de se déclarer tout autant compétents pour connaître d'un même litige.

594. Compte tenu de la nature et du processus du *spamming*, mais également de la diversité des menaces qui sévissent à différents stades, il nous est paru utile de rechercher une protection efficace du « spammé » sur un double front : d'une part, sur le terrain de la protection des données et, d'autre part, sur celui de la réglementation des expéditions des messages. Cela nous a conduit, dans un premier temps, a interrogé les lois spéciales existantes, à savoir : la loi informatique, fichiers et libertés dont l'ambition est d'encadrer l'exploitation des données à caractère personnel et la loi pour la confiance dans l'économie numérique qui a vocation, notamment, à encadrer les envois commerciaux et, à cette fin, prohibe la pratique du *spamming*. La mise en œuvre ou l'application de ces lois spéciales a permis de révéler leurs carences et leur insuffisance à assurer une protection pleinement satisfaisante des « spammés ». La confrontation du *spamming* à l'ensemble des dispositions relatives à la protection des données à caractère personnel a permis de mettre en exergue les limites de cette législation, tant dans sa fonction curative que préventive. Son application doit également être mise en cause : les sanctions peu dissuasives qui ont été prononcées dans les rares décisions recensées en témoignent. Les dispositions législatives spécialement adoptées pour lutter contre le *spamming* ont également échoué. Les raisons de cet échec sont dues à l'incapacité pour la loi, d'un côté, à appréhender le phénomène du *spamming* comme un ensemble de pratiques diverses, multiples et évolutives et, de l'autre côté, à assurer une protection juridique efficace (c'est-à-dire dissuasive) à l'ensemble des « spammés ». Au-delà de cette analyse, la dimension internationale du *spamming* imposait de déterminer le niveau de protection existant au-delà de nos frontières. La comparaison du droit français et du droit américain a été particulièrement instructive. Déceler les divergences opposant ces deux systèmes juridiques nous a permis de mesurer les difficultés à entrevoir en présence d'un litige de dimension internationale. Nous avons tenu à souligner que de telles oppositions risquaient de compromettre l'efficacité des solutions issues d'un droit interne exposé à la concurrence de droits étrangers susceptibles de se déclarer tout aussi compétents pour connaître d'un même litige.

595. Pour tenter de dépasser l'ensemble de ces lacunes, nous avons fait appel au droit pénal. La dangerosité du *spamming*, illustrée notamment à travers le *mail bombing*, le *phishing* ou la transmission de virus, imposait la recherche de fondements juridiques capables d'engager la responsabilité pénale des « spammeurs ». Notre analyse nous a permis de conclure que le droit pénal offrait des fondements intéressants pour combler certaines des lacunes révélées par la mise en œuvre des lois spéciales. En premier lieu, le droit pénal de l'informatique permettra d'engager la responsabilité du « spammeur » chaque fois que les envois de *spams* portent atteinte au système de traitement automatisé de données. Tel sera le

cas dans les hypothèses de *mail bombing* ou lorsque le « spammeur » prend le contrôle d'un ordinateur à l'insu de son propriétaire pour procéder à l'envoi de *spams*. Le droit pénal de l'informatique pourra encore être sollicité lorsque le *spamming* est le vecteur d'actions frauduleuses sur les données, en particulier lorsqu'il est porteur de virus destiné à infecter l'ordinateur de la victime. En deuxième lieu, le droit pénal de la consommation garantit la sanction des contenus commerciaux trompeurs, ce que la Lcen n'envisage pas. Enfin, le délit d'escroquerie offre une autre voie de condamnation, lorsque des contenus frauduleux tendent à obtenir insidieusement la remise de données nominatives ou de sommes d'argent. La mise en œuvre des dispositions relatives à l'escroquerie devrait offrir une sanction efficace contre l'association du *spamming* et du *phishing.* Malgré les vertus que pourrait comporter la mise en œuvre de ces différents délits, nous avons constaté, avec regret, que le droit pénal demeurait insuffisamment exploité, sauf à considérer de rares décisions intervenues pour sanctionner des cas de *mail bombing* ou d'attaque par PC zombie. C'est un constat que nous déplorons mais gageons que devant les intérêts personnels et les enjeux d'ordre public, les victimes du *spamming* et les autorités chargées de combattre cette pratique poursuivront leurs agresseurs devant les juridictions pénales, seules en mesure de sanctionner, avec la pertinence et la détermination nécessaires, des comportements répressifs que les lois spéciales ne parviennent pas à menacer. Par ailleurs les dommages causés par l'envoi de *spams* nécessitait d'interroger le droit de la responsabilité civile, d'une part délictuelle et d'autre part contractuelle. Concernant l'efficacité de cette dernière, si la résiliation est apparue comme une sanction radicale permettant de faire cesser le *spamming*, celle-ci s'est révélée d'un effet très limité puisque d'une part seul le FAI avec lequel le « spammeur » a conclu un contrat pourra agir sur ce fondement et d'autre part, pourra toujours contracter avec un autre FAI. S'agissant de l'action en responsabilité civile, s'il est apparu qu'en théorie, les « spammés » pouvaient assez aisément rapporter la preuve de la responsabilité du « spammeur », cette action a toutefois révélé ses limites au stade de la réparation, en particulier lorsque les « spammés » ne subissent qu'un préjudice minime. Pour surmonter ces difficultés, nous avons donc recherché des solutions qui permettraient de faire évoluer notre droit de la responsabilité civile délictuelle afin de le rendre plus efficace. Les évolutions proposées ont porté à la fois sur le droit substantiel mais aussi sur le droit processuel. S'agissant du droit substantiel, nous avons démontré que la reconnaissance de la faute lucrative en droit de la responsabilité civile permettrait de prendre en compte des comportements, comme le *spamming,* qui restent pour le moment insuffisamment poursuivis. L'éventuelle consécration de ce type de faute par le droit de la responsabilité civile nous a conduits naturellement à envisager la question de sa sanction. À cet égard, les enseignements de droit comparé ont été très riches. À l'instar du droit américain, l'introduction des

dommages-intérêts punitifs dans notre droit est apparue comme particulièrement adaptée pour sanctionner ce type de faute puisque seul l'effacement des profits réalisés pourrait permettre de punir efficacement les responsables et notamment les « spammeurs ». Cette proposition induirait inéluctablement de faire évoluer la fonction traditionnellement réparatrice de l'action en responsabilité civile délictuelle vers une fonction répressive. Toutefois, à l'examen de la pratique actuelle des juges dans certaines affaires et de certaines dispositions légales, cet aménagement n'apparaîtrait pas impossible. S'agissant du droit processuel, il est apparu essentiel de faire cesser une situation intolérable où un grand nombre de « spammeurs » continuent à profiter d'une activité particulièrement lucrative au préjudice de milliers de personnes. La reconnaissance d'une action de groupe, inspirée de la *class action* américaine, est apparue à cette fin particulièrement pertinente pour tous les « spammés » dont le dommage est trop minime pour engager, seules, une telle action. Cette proposition permettrait ainsi d'offrir une réponse pertinente à l'impunité dont bénéficient trop de « spammeurs ».

596. Au-delà de cette démarche strictement nationale, le second volet de cette recherche ne pouvait ignorer le contexte international dans lequel est baignée la problématique du spamming. En effet, la question de l'effectivité du droit français dans ce contexte ne pouvait être ignorée. Les conflits de lois et de juridictions que suscitent toute situation de *spamming* impliquant un élément d'extranéité imposait d'emprunter la démarche adoptée en droit international privé afin de permettre de désigner une loi et une juridiction compétentes. Le droit international privé a permis, au moins partiellement, d'offrir certaines réponses dans les hypothèses de *spamming* les plus simples où le fait générateur et le dommage sont localisés dans des pays distincts. Les limites des solutions issues des règles de conflit classiques se sont manifestées dans les cas de *spamming* les plus complexes, c'est-à-dire lorsque le lieu de localisation du fait générateur et/ou de celui du dommage ne sont plus uniques. Ces insuffisances se sont révélées tant en matière de compétence juridictionnelle que législative. Afin de surmonter ces difficultés, nous avons été conduits à rechercher alors une règle de conflit qui serait propre au *spamming.* La résidence du « spammé » est ainsi apparue comme un rattachement pertinent non seulement pour la compétence juridictionnelle mais aussi pour la compétence législative. Au-delà des principaux avantages qu'elle présente d'un point de vue pratique ; l'identification d'un critère commun à ces deux compétences permettrait de faciliter la mise en œuvre d'un droit national par ses propres juridictions, les compétences étant en pratique souvent liées.

597. Vers d'autres orientations. Le rapport entre le *spamming* et le droit est un sujet très riche comme nous avons pu le constater et qui reste une source de réflexions loin d'être épuisée. En effet, notre étude consistait à rechercher les fondements juridiques permettant au « spammé » de poursuivre le « spammeur » dans diverses hypothèses. Seule la relation « spammeur »/« spammé » intéressait donc notre analyse. Toutefois, au-delà de ce champ d'investigations, une lutte effective contre le *spamming* nécessiterait également d'engager une réflexion orientée vers une perspective plus large qui consisterait à prendre en compte cette fois l'impact global de cette pratique. Afin de mesurer l'intérêt de cette nouvelle piste de réflexions, arrêtons-nous quelques instants sur cette hypothèse. Au regard de l'impact global du *spamming* [1784], cette pratique compte parmi ces nouvelles « plaies du *Web* » qui polluent l'environnement numérique et contribuent à ternir l'image des services de communications électroniques en ralentissant, voire en paralysant les échanges d'informations. Cette analogie entre le *spamming* et la pollution n'est pas anodine et nous conduit naturellement à explorer une voie pourtant inhabituelle pour régler les problèmes induits par les nouvelles technologies, à savoir le droit de l'environnement et les instruments juridiques déjà existants destinés à assainir un environnement menacé.

598. La pollution, une externalité négative. L'économiste Arthur Cecil PIGOU est considéré comme le père fondateur de cette notion d'externalité [1785] qui peut se définir comme *« l'effet de la décision d'une personne sur une autre personne non-partie prenante à cette décision »* [1786]. Autrement dit, il existe une externalité lorsque l'activité d'une personne influence le bien-être d'une autre personne sans que cette dernière ne reçoive ni ne paie aucune compensation pour cet effet. Lorsque que cet effet est défavorable, on parle d'externalité négative. Une externalité négative, encore appelée **«** déséconomie externe », existe dès lors qu'un acteur économique fait supporter un coût à un ou plusieurs autres agents, sans que le premier n'ait à payer pour le coût qu'il fait ressentir aux autres [1787]. Tel est le cas de la pollution. Les externalités externes provoquent ainsi d'une part un coût social non compensé et imposé à la collectivité sans aucune transaction volontaire et constituent d'autre part un défaut du marché qui se traduit par des conflits d'intérêts entre agents économiques sans que ces conflits s'expriment directement en terme monétaire. Afin de

[1784] C'est-à-dire les coûts du *spamming* pour les entreprises et les FAI, ralentissement du fonctionnement des services de messagerie, encombrement de la bande passante des FAI … (V. *supra : intro*).
[1785] Arthur Cecil PIGOU, *The Economics of Welfare*, 4ème éd., Macmillan and Co Limited, London, 1960.
[1786] Ronald H. COASE, *La firme, le marché et le droit*, Diderot, Paris, 1997, p. 33. – c'est-à-dire que toutes actions, transactions ou autres opérations sont susceptibles d'avoir des répercussions sur des tiers. Selon un autre auteur, les externalités *« résultent des conséquences des décisions d'un agent qui affectent d'autres agents autrement que par le marché »* (J. Bremond, *Les économistes néoclassiques*, 2e éd., Hatier, 1989, p.81).
[1787] Cet effet passe en général par la dégradation d'une ressource naturelle dont les autres agents sont utilisateurs. Le coût qui existe est bien un coût externe, extérieur à l'agent qui en est à l'origine.

démontrer en quoi l'externalité correspond à des divergences entre les coûts privés et les coûts sociaux liés à une activité économique, PIGOU s'appuie sur une situation où des individus extérieurs au processus de production en sont affectés [1788]. Il en est ainsi dans le cas où « *l'essence du problème est qu'une personne A, au moment de rendre un service, moyennant paiement, à une autre personne B, procure de manière incidente un service ou un désavantage à d'autres personnes (non producteurs de services identiques) de telle sorte qu'aucun paiement ne peut être exigé de la partie bénéficiaire ou qu'aucune compensation ne peut être imposée au profit de la partie lésée.* »

599. L'exemple du *spamming*. Dans le cas du *spamming*, un FAI fournit au « spammeur » la possibilité d'accéder à une connexion à l'internet par le biais d'un contrat. Ce lien contractuel permet au « spammeur » de bénéficier des services de messagerie électronique grâce auxquels il pourra procéder à l'expédition de *spams*, opération d'envoi qui créera dans le même temps un désavantage pour les internautes qui supporteront les coûts liés à la réception de *spams*. Il se crée ainsi un déséquilibre entre le « spammeur » qui échappera aux coûts des envois et les destinataires sur lesquels ces derniers sont répercutés. Le coût inhérent aux *spams* que doivent supporter les internautes devient supérieur au coût de production à la charge du « spammeur », créant ainsi une externalité négative. Ce coût « social » inclut les coûts que le « spammeur » devrait normalement supporter auquel s'ajoute le coût lié aux mesures qui devront être prises par l'ensemble des internautes affectés par cette pollution pour assainir cette situation. À titre d'exemple, la réception massive de *spams* par un FAI le contraindra notamment à engager des dépenses afin d'élargir sa bande passante et acquérir des mesures techniques, notamment des filtres destinés à contrer cette pollution. Il en résulte que les coûts sociaux deviennent supérieurs aux bénéfices sociaux générés par la production de *spams*, laissant apparaître un déséquilibre entre ce que procure le *spam* et ce qu'il en coûte aux internautes. En ce sens, la production de *spams* devient alors inefficace pour la société. C'est dans ce contexte qu'il apparaît essentiel de proposer une solution destinée à rétablir un équilibre entre les coûts réels que doit supporter la société et ceux que doit assumer le « spammeur ».

600. L'internalisation des externalités négatives. Pour corriger ce déséquilibre PIGOU a proposé d'internaliser les externalités externes, c'est-à-dire leur associer un quasi-

[1788] Trois catégories de personnes peuvent en réalité correspondre à cette situation où se crée une externalité, un défaut du marché. Pour nos développements, seul l'un d'entre eux sera ici développé car il permet de comprendre la pertinence de l'utilisation de cette notion d'économie en matière de spamming, l'avantage que retire un spammeur de son activité et ce, au détriment des internautes. Pour plus de détails, consulter la thèse de Elzéar DE SABRAN-PONTEVES, *Les transcriptions juridiques du principe du pollueur-payeur*, 2004, Aix Marseille III, spéc. p. 182.

prix [1789]. L'objectif de l'internalisation est de parvenir à ce que le pollueur intègre dans les coûts de sa production celui de l'atteinte aux biens environnementaux. Elle consiste donc à faire payer au pollueur le dommage environnemental dont il est responsable. En faisant supporter aux responsables les effets externes de leurs actions, l'objectif final de l'internalisation des externalités est d'aboutir à une modification des comportements en leur faisant prendre conscience des conséquences de leurs actions. Pour tenter de rétablir cet équilibre dans l'environnement matériel, le droit de l'environnement dispose d'un instrument intéressant, à savoir le principe du « pollueur-payeur » [1790] qui constitue l'« *expression juridique de l'instrument économique d'internalisation des coûts sociaux* » [1791]. En effet, source d'inefficacité pour la société, la pollution doit disparaître ou plus rationnellement doit être limitée en internalisant les coûts de pollution. [1792]. En quelques mots, ce principe consiste schématiquement, à ce que « celui qui pollue, est celui qui doit payer ». Selon ce principe, la production d'un bien ou d'un service peut provoquer un certain nombre d'effets externes qui ne sont pas pris en compte par le marché mais qu'il est nécessaire d'intégrer dans le prix du bien ou du service en les imputant à ceux qui en sont à l'origine [1793]. Ce principe postule que les coûts de lutte contre la pollution doivent être supportés directement par les pollueurs bien qu'ils pourraient tout à fait les répercuter sur les consommateurs dans un second temps. En tout état de cause, l'intégration du coût de la pollution dans les coûts de production est généralement réalisée par le biais de la taxation du responsable de la pollution [1794].

601. Les vertus des instruments fiscaux en matière de *spamming.* Comme nous l'avons souligné à plusieurs reprises, le succès du *spamming* tient, pour l'essentiel, à son

[1789] Ce n'est pas un vrai prix puisqu'il n'existe pas de marché mais la monnaie constitue le seul instrument de mesure existant dans la vie sociale.

[1790] -Ar. L.110-1 du C. de l'environnement : « *les frais résultant des mesures de prévention, de réduction de la pollution et de lutte contre celle-ci sont supportés par le pollueur* ». Ce principe figure également parmi les principes fondateurs du droit communautaire de l'environnement énumérés à l'article 174.2 du traité instituant la Communauté européenne. – La fonction du principe du pollueur-payeur, défini pour la première fois et recommandé par l'OCDE depuis 1972 (Recommandation du Conseil sur les principes relatifs aux aspects économiques des politiques de l'environnement sur le plan international, adoptée par le Conseil lors de sa 293ème séance, le 26 mai 1972, in Le principe du pollueur-payeur, OCDE, Paris, 1975, pp.9-12. Annexe 1), constitue le véritable acte fondateur de ce principe et surtout de l'approche économique des questions environnementales, cadre plus général dans lequel il s'insère. Il ne s'agit pas d'un principe juridique d'équité mais un principe d'efficacité économique.

[1791] A. PETITPIERRE-SAUVAIN, « Le principe du pollueur-payeur en relation avec la responsabilité du pollueur », Zeitschrift für Schweirerisches Recht, 4. Heft, Halbband II 1989, spéc. p. 443.

[1792] A. PETITPIERRE-SAUVAIN, « Le principe du pollueur-payeur en relation avec la responsabilité du pollueur », *op. cit.*, spéc. p. 447 (Le recours à l'instrument économique d'internalisation des coûts externes peut constituer une solution efficace pour permettre de corriger les effets externes négatifs (externalités) *« en rabattant les coûts résultant des atteintes à l'environnement dans la sphère d'un auteur particulier à qui ces atteintes sont attribuées, on amène celui-ci à les intégrer dans un calcul économique…* »).

[1793] N. DE SADELEER, *Le droit communautaire des déchets*, L.G.D.J., Bruyant Bruxelles, 1995, p. 521

[1794] PIGOU fut l'un des premiers partisans, sert à corriger les effets d'une externalité négative (« taxe pigouvienne »).

caractère très lucratif puisqu'il permet que le coût des envois se répercute exclusivement sur les destinataires. Cette situation crée indéniablement un déséquilibre économique conséquent au sein de la communauté des internautes. Or, « [l]*a stratégie la plus efficace pour modifier le comportement de ceux qui sur Internet, ne respectent pas les droits et libertés des personnes consiste à taper sur le point faible, c'est-à-dire le « portefeuille » des entreprises* »[1795]. La création d'une taxe sur le *spamming* permettrait de corriger ce déséquilibre en internalisant, c'est-à-dire en faisant peser sur les « spammeurs » les coûts écologiques qu'ils avaient pour habitude de répercuter sur l'ensemble de la collectivité cybernétique [1796]. Les instruments économiques pourraient ainsi, à la différence des normes réglementaires [1797] exercer une véritable pression en permanence sur le portefeuille des « spammeurs » qui restaient jusqu'alors intouchables. L'objectif est clair : il s'agit de mener les « spammeurs » à modifier leur comportement et à les décourager face à cet engouement croissant pour le *spamming* en supprimant l'avantage économique qu'ils pouvaient en retirer. Selon cette option, les « spammeurs » devraient ainsi payer un certain montant de taxe par envoi de *spams*, ce qui les inciterait à réduire d'eux-mêmes le niveau de *spams*. Adopter un comportement plus « sain » dans l'environnement numérique lui permettrait ainsi de diminuer le montant de la taxe à payer. Encore faut-il toutefois que ce taux de taxation soit correctement fixé, c'est-à-dire égal au coût de l'externalité. Pour cela, il doit être suffisamment élevé pour inciter les « spammeurs » à diminuer le taux d'envois de spams car à défaut, cette taxe ne permettra pas d'éliminer cette distorsion qui existe sur le marché, tout en s'assurant que ce taux ne soit pas non plus excessif, sous peine de substituer une distorsion à une autre sans aucun résultat palpable. Cette solution apparaît intéressante pour tenter de paralyser les avantages économiques qui motivent les « spammeurs » à poursuivre leurs pratiques [1798]. En effet, en annulant l'avantage escompté, l'intérêt attaché à l'envoi de *spams* s'en trouvera inévitablement amoindri et le nombre de *spams* sera de ce fait

[1795] Jean FRAYSSINET, *« La protection des données personnelles est-elle assurée sur Internet ? »*, intervention lors du colloque international *Droit et Internet. Approches européennes et internationales*, 19-20 nov. 2001 (disponible sur le site de Paris I).

[1796] Sur la taxation du spam, voir : Derek E. BAMBAUER *Solving the Inbox Paradox : An Information-Based Policy Approach to Unsolicited E-Mail Advertising*, Virginia Journal of Law & Technology Vol.10, n°5 (2005) : §164 Le but serait de forcer les consommateurs à être plus conscients du coût d'évaluation, de leurs achats par la publicité par courrier non sollicité et d'allouer de façon plus égale les bénéfices et le poids du spam. Le spam crée souvent une externalité. Il bénéficie aux « récepteurs » qui évaluent l'information ou qui l'utilisent pour initier leurs achats mais imposent des coûts sur les autres. Les parties qui bénéficient d'une transaction initiée ou consommée par la publicité par e-mail non sollicitée ne supportent pas le coût « sociétal » du spam parce que les expéditeurs peuvent transférer à un prix très bas un simple message à plusieurs destinataires, seulement peu d'entre eux peuvent évaluer l'information du message.

[1797] Les normes réglementaires fixent généralement un seuil à ne pas dépasser et n'incite donc pas suffisamment les pollueurs à diminuer de façon significative leur volume de courriers polluants puisque celui qui s'approche au plus près du niveau de pollution zéro ne retirera pas plus d'avantages que celui qui se contente de rester tout juste sous le seuil limite autorisé.

[1798] V. en ce sens Guillaume TEISSONNIERE, « La lutte contre le spamming : de la confiance en l'économie numérique à la méfiance envers ses acteurs », http://www.juriscom.net/documents/spam20040402.pdf.

certainement réduit. Par ailleurs, un certain équilibre sera rétabli dans « l'écosystème numérique » entre les acteurs à l'origine du *spam* et les personnes en subissant les effets. L'internalisation des externalités vise donc à rétablir un équilibre économique que les « spammeurs » ont brisé en se soustrayant à la charge financière qui leur incombait logiquement. Une telle mesure pourrait notamment s'inspirer de la loi de finances rectificative pour 2003 qui vient de consacrer l'application du principe du pollueur-payeur au publipostage « papier » non sollicités [1799].

602. Ainsi, brièvement exposée, la problématique environnementale du *spamming* offre d'intéressantes perspectives en matière de lutte anti-*spam*. Espérons qu'une étude explorant ce nouveau champ de recherches soit entreprise dans un avenir proche.

[1799] L'article 16bis de la loi de finances rectificatives pour 2003 insère un nouvel article L.541-10-1 dans le Code de l'environnement ainsi rédigé : « À compter du 1er janvier 2005, toute personne physique ou morale qui, gratuitement, met pour son propre compte à disposition des particuliers sans que ceux-ci en aient fait préalablement la demande, leur fait mettre à disposition, leur distribue pour son propre compte ou leur fait distribuer des imprimés nominatifs, dans les boites aux lettres, dans les parties communes des habitations collectives, dans les locaux commerciaux, dans les lieux publics ou sur la voie publique est tenue de contribuer à la collecte, la valorisation et l'élimination des déchets ainsi produits ».

BIBLIOGRAPHIE

OUVRAGES GENERAUX, TRAITES, MANUELS, COURS

AUBERT (J.-L.) et (É.) SAVAUX
Introduction au droit et thèmes fondamentaux du droit civil, 13e éd., Sirey, 2010.

AUDIT (B.)
Droit international privé, 5e éd., Economica, coll. *Corpus Droit Privé*, 2008.

BATIFFOL (H.)
Aspects philosophiques du droit international privé, Dalloz, coll. *Philosophie du droit*, 1956.

BENABANT (A.)
Droit civil : Les obligations, 12e éd., Montchrétien, coll. *Domat Droit privé*, 2010.

BERGEL (J.-L.)
Méthodologie juridique, 1re éd., P.U.F., coll. *Thémis droit privé*, 2001.

BERGEL (J. -L.), BRUSCHI (M.) ET CIMAMONTI (S.)
Traité de droit civil : Les biens, (sous la dir. Jacques GHESTIN), 2e éd., L.G.D.J., 2010.

BOULOC (B.)
Droit pénal général, 21e éd., Dalloz, coll. *Précis*, 2009.

BOUREL (P.)
Du rattachement de quelques délits spéciaux en droit international privé français, *RCADI* 1989, tome 214.

BUFFELAN-LANORE (Y.) et LARRIBAU-TERNEYRE (V.)
Droit civil : Les obligations, 12e éd., Dalloz Sirey, 2010.

BUREAU (D.) et MUIR WATT (H.)
Droit international privé, tome 1 (Partie générale), 2e éd., PUF, coll. *Thémis Droit*, 2010
Droit international privé, tome 2 (Partie spéciale), 2e éd., PUF, coll. *Thémis Droit*, 2010.

CARBONNIER (J.)
- *Droit civil : Les obligations*, tome 4, 22e éd. refondue, P.U.F, coll. *Thémis droit privé*, 2000.
- Droit civil : *Les personnes*, tome 1, P.U.F., coll. *Thémis droit privé*, 2000
- *Droit civil, Introduction*, 27e éd., P.U.F., 2002.

CHABAS (F.) et LAROCHE-GISSEROT (F.)
- *Les personnes – La personnalité – Les incapacités*, tome 1, vol. 2, 6e éd., Montchrétien, coll.
- *Leçons de droit civil Henri, Jean et Léon MAZEAUD*, 1997.

CHARTIER (Y.)
La réparation du préjudice dans la responsabilité civile, Dalloz, 1996.

COUTANT-LAPALUS (C.)
Le principe de la réparation intégrale en droit privé, (préf. Frédéric POLLAUD-DULIAN), P.U.A.M., 2002.

DELEBECQUE (Ph.)

Droit des obligations : Contrat et quasi-contrat, tome 1, 4e éd., Litec, coll. *Objectif droit cours,* 2007.

DESPORTES (F.) et LE GUNEHEC (F.)
Droit pénal général, 16e éd., Economica, coll. *Corpus Droit privé,* 2009.

FABRE-MAGNAN (M.)
- *Droit des obligations : Responsabilité civile et quasi-contrats*, P.U.F, coll. *Thémis droit,* 2010.
- *Droit des obligations : Contrat et engagement unilatéral,* 2e éd., P.U.F, coll. *Thémis droit,* 2010.

FLOUR (J.), AUBERT (J.-L.) et SAVAUX (É.)
- *Les obligations* : *Le fait juridique,* tome 2, 13e éd., Sirey, coll. *Sirey Université,* 2009.
- *Les obligations : Le rapport d'obligations,* tome 3, Sirey, coll. *Sirey Université,* 2009.

GAUDEMET-TALLON (H.)
Le pluralisme en droit international privé : Richesses et faiblesses (Le funambule de l'arc-en-ciel), RCADI 2005, tome 312.

GHESTIN (J.) et GOUBEAUX (G.)
Traité de droit civil : Introduction générale, 4e éd. avec le concours de Muriel FABRE-MAGNAN, L.G.D.J., 1995.

MALAURIE (P.), AYNES (L.) et STOFFEL-MUNCK (P.)
Droit civil : Les obligations, 4e éd., Defrénois, 2009.

LAGARDE (P.)
Le principe de proximité dans le droit international privé contemporain, RCADI 1986, tome 196.

LAITHIER (Y.-M.)
Droit comparé, Dalloz, coll. *Cours,* 2009.

LARROUMET (C.)
Les obligations : Le contrat, 2ème partie : Les effets, 4e éd., Économica, 2007.

LOUSSOUARN (Y.), BOUREL (P.) et DE VAREILLES-SOMMIERES (P.)
Droit international privé, 9e éd., *Dalloz,* 2007.

MALAURIE (P.) et AYNES (L.)
Philippe MALAURIE et Laurent AYNES, *Cours de droit civil : Les contrats spéciaux,* 14e éd., Cujas, 2001.

MALAURIE (P.) et MORVAN (P.)
Introduction générale, 3e éd., Defrénois, 2009

MAYER (P.) et HEUZE (V.)
Droit international privé, 10e éd., Montchrétien, coll. *Domat droit privé,* 2010.
Droit international privé, 9e éd., Montchrestien, 2007.

MAZEAUD (H.), (L.) et (J.)
Traité théorique et pratique de la responsabilité civile délictuelle et contractuelle, tome 2, 6e éd., Montchrestien, 1970.

MAZEAUD (H. et L.) et TUNC (A.)
Traité théorique et pratique de la responsabilité civile délictuelle et contractuelle, (préf. Henri CAPITANT), tome 1, 6e éd., Montchrétien, 1965.

MAZEAUD (H). et (L.), MAZEAUD (J.) et CHABAS (F.)
- *Leçons de droit civil, Obligations : théorie générale*, tome 2, vol. 1, 9e éd., par François CHABAS, Montchrétien, 1998.
- *Traité théorique et pratique de la responsabilité civile délictuelle et contractuelle*, (préf. Henri CAPITANT), tome 3, vol. 1, 6e éd., Montchrétien, 1978.

NIBOYET (M.-L.) et DE GEOUFFRE DE LA PRADELLE (G.)
Droit international privé, 2e éd., L.G.D.J., coll. *Manuel*, 2009.

PRADEL (J.)
Droit pénal général, 18e éd., Cujas, coll. *Référence*, 2010

PRADEL (J.) et DANTI-JUAN (M.)
Droit pénal spécial, 5e éd., Cujas, coll. *Référence*, 2010.

SACCO (R.)
La comparaison juridique au service de la connaissance du droit, Economica, coll. *Études juridiques comparatives*, 1991.

STARK (B.), ROLAND (H.) et BOYER (L.)
Obligations : Responsabilité délictuelle, tome 1, 5e éd., Litec, 1996.

TERRE (F.)
Introduction générale au droit, 8e éd., Dalloz, coll. *Précis*, 2009.

TERRE (F.), SIMLER (P.) et LEQUETTE (Y.)
Droit civil : Les obligations, 10e éd., Dalloz, coll. *Précis droit privé*, 2009.

VERON (M.)
Droit pénal spécial, 13e éd., Dalloz-Sirey, coll. *Sirey Université*, 2010.

VIGNON-BARRAULT (A.)
Intention et responsabilité civile, (préf. Denis MAZEAUD), P.U.A.M., coll. *Institut de Droit des Affaires*, 2004.

VINEY (G.)
- *Introduction à la responsabilité : évolution générale, responsabilité civile et responsabilité pénale, responsabilité contractuelle et responsabilité délictuelle*, (sous la dir. de Jacques GHESTIN), 2e éd., L.G.D.J., 1995.
- *Introduction à la responsabilité*, 3e éd., L.G.D.J., coll. *Traité de droit civil*, 2008.

VINEY (G.) et JOURDAIN (P.)
Traité de droit civil : Les conditions de la responsabilité, (sous la dir. de Jacques GHESTIN), 3e éd., L.G.D.J., 2006.

ALBIGÈS (C.), ARTZ (J.-F.), BADENAS CARPIO (J.-M.) et al.
Études du droit de la consommation, Liber Amicorum Jean CALAIS-AULOY, Dalloz, coll. *Mélanges,* 2004.

ALEIX SANTURE (M.), ARSEGUEL (A.), AUDECOUD (O.) et al.
Mélanges Laurent BOYER, (préf. Roger MERLE), Presse universitaire des Sc. Soc. de Toulouse I, 1996.

AMIAUD (A.), BECQUE (É.), CHAUVEAU (P.), et al.
Le droit privé au milieu du XX^e siècle, Études offertes au professeur RIPERT, tome 2, L.G.D.J., coll. *Mélanges,* 1950.

AMIEL-DONAT (J.), ATIAS (C.), BIBENT (M.) et al.
Mélanges André Colomer, Litec, Paris, 1993.

AMLON (G.), ANCEL (M.-É), ANCEL (P.) et al.
Prospectives du droit économique, Dialogues avec Michel JEANTIN, (préf. Jean CARBONNIER), Dalloz, 1999.

ANCEL (M.-É), BEKERMAN (G.), BERTRAND (A. R.) et al.
Droit et technique – Études à la mémoire du professeur Xavier Linant de Bellefonds, Litec – LexisNexis, coll. *Les Mélanges,* 2007.

ANCEL (B.) et LEQUETTE (Y.)
Les grands arrêts de la jurisprudence française de droit international privé, Dalloz, 5^e éd. 2006.

ANTAKI (N.), BEGUIN (J.), BOULOC (B.) et al.
Aspects actuels du droit des affaires, Mélanges en l'honneur de Yves Guyon, Dalloz, 2003.

AUDIER (J.), BERGEL (J.-L.), BONASSIES (P.) et al.
Études offertes à Pierre KAYSER, (préf. Charles DESBBASH), tome 1, P.U.F., 1979.

BEN ACHOUR (R.) et LAGHMANI (S.) (sous la dir.)
Le droit international face aux nouvelles technologies, Colloque des 11, 12 et 13 avril 2002, éd. A. Pedone, coll. *Rencontres internationales de la faculté des sciences juridiques, politiques et sociales de Tunis,* 2002.

BOELE-WOELKI (K.) et KESSEDJIAN (C.) (sous la dir.)
Internet Which Court Decides ? Which Law Applies ? Quel tribunal décide ? Quel droit s'applique ?, Kluwer Law International, Law and Electronic Commerce, vol. 5, 1998.

BRUGUIERE (J.-M.), MALLET-POUJOL (N.) et ROBIN (A.) (sous la dir.)
Propriété intellectuelle et droit commun, P.U.A.M., coll. *Institut de droit des affaires,* 2007.

CARTWRIGHT (J.), VOGENAUER (S.) et WHITTAKER (S.) (sous la dir.)
Regards comparatistes sur l'avant-projet de réforme du droit des obligations et de la prescription, Société de législation comparée, coll. *Droit privé comparé et européen,* vol. 9, 2010.

CATALA (P.), CHARLEMAGNE (P.), BOUCOURECHLIEV (J.) et al.

Droit et informatique : L'hermine et la puce, (préf. Jean CARBONNIER), Masson, coll. *Frederick R. Bull,* 1992.

CHATILLON (G.) (sous la dir.)
Le droit international de l'Internet, Bruylant, Bruxelles, 2001.

CORNU (G.)
Vocabulaire juridique, Ass. H. CAPITANT, 8e éd., Quadridge-PUF, 2007.

DELMAS-MARTY (M.) (sous la dir.)
Critique de l'intégration normative : L'apport du droit comparé à l'harmonisation des droits, P.U.F., coll. *Les voies du droit,* 2004.

FABRE-MAGNAN (M.), GHESTIN (J.), JOURDAIN (P.) et al.
Liber Amicorum, Études offertes à Geneviève VINEY, L.G.D.J.-Lextenso, coll. *Les Mélanges,* 2008.

FOYER (J.), LARGUIER (J.), SCHMIDT (J.) et al.
Les Droits et le Droit, Mélanges dédiés à Bernard BOULOC, Dalloz, 2007.

GOUBEAUX (G.), GUYON (Y.), JAMIN (C.) et al. (sous la dir.)
Le contrat au début du XXIe siècle, Études offertes à Jacques GHESTIN, L.G.D.J., 2001.

GUINCHARD (S.) et DEBARD (TH.)
Lexique des termes juridiques, 18e éd., Dalloz, 2011.

LE DOUARIN (N. M.) (sous la dir.)
Science, éthique et droit, (préf. Claude ALLEGRE, postface François TERRE), Odile Jacob, 2007.

LE TOURNEAU (P.) (sous la dir.)
- *Droit de la responsabilité et des contrats,* 6e éd., Dalloz, coll. *Dalloz Action,* 2006.
- *Droit de la responsabilité et des contrats,* 8e éd., Dalloz, coll. *Dalloz Action,* 2010.

ATIAS (C.), BADINTER (R.), BERGEL (J.-L.) et al.
Le droit privé français à la fin du XXe siècle, Études offertes à Pierre CATALA, Litec, coll. *Les Traités,* 2001.

LOQUIN (É.) et Anie MARTIN (A.) (sous la dir.)
Droit et marchandisation, Litec, Paris, 2010.

LOUSSOUARN (Y.) et LAGARDE (P.) (sous la dir.)
L'information en droit privé. Travaux de la conférence d'agrégation, L.G.D.J., coll. *Bibl. dr. privé,* 1978.

MALINVAUD (P.) (président de l'association)
Le renouvellement des sources du droit des obligations. – Journées nationales. Lille-1996, tome 1/Lille-1996, L.G.D.J., Ass. H. Capitant, 1997.

MONTERO (É), DHONT (J.), FESLER (D.) et al.
Le droit des affaires en évolution : Le contrat sans papier, Bruylant-Kluwer, Bruxelles-Antwerpen, 2003.

Mélanges offerts à Jacques Maury, tome 1, Dalloz-Sirey, 1960.

NUYTS (A.) (sous la dir.)
International Litigation in Intellectual Property and Information Technology, Kluwer Law International, 2008.

PEDROT(P.) (sous la dir.)
Traçabilité et responsabilité, Economica, 2003.

PIATTI (M.-C.) (sous la dir.)
Les libertés individuelles à l'épreuve des NTIC, P.U.L., 2001.

PIGNARRE (G.) (sous la dir.)
Forces subversives et forces créatrices en droit des obligations : *Rétrospective et perspectives à l'heure du Bicentenaire du code civil,* Dalloz, 2005.

POUSSON-PETIT (J.) (sous la dir.)
L'identité de la personne humaine – Etude de droit français et de droit comparé, Bruylant, 2002.

SAINTOURENS (B.) (sous la dir.)
Le Code civil, une leçon de légistique ?, Economica, coll. *Études juridiques*, 2006.

TABATONI (P.) (sous la dir.)
La protection de la vie privée dans la société de l'information, P.U.F, coll. *Cahiers sciences morales,* Paris, 2002.

CHARLOTTE WAELDE (sous la dir.de)
Law and the Internet, Hart Publishing, 2009.

OUVRAGES SPECIAUX, THESES, MEMOIRES, ENCYCLOPEDIE

ANDORNO (R.)
La distinction juridique entre les personnes et les choses : À l'épreuve des procréations artificielles, (préf. François CHABAS), tome 263, LGDJ, coll. *Bibliothèque de droit privé,* 1996.

AOUN (F.) ET RASLE (B.)
Halte au spam, éd. Eyrolles. 2003.

BALLANDRAS ROZET (C.)
Les techniques conventionnelles de lutte contre les pollutions et les nuisances et de prévention des risques technologiques, Université Jean Moulin – Lyon 3 – Faculté de Droit, 29 novembre 2005.

BERG (O.)
La protection des intérêts incorporels en droit de la réparation des dommages : Essai d'une théorie en droit français et allemand, (préf. Geneviève VINEY), Bruyland- L.G.D.J., 2006.

BITAN (F.)
Courrier Électronique, J.-Cl. Communication, Fasc. 4740, 2006.

BOELE-WOELKI (K.) et KESSEDJIAN (C.) (sous la dir.)

Internet : Which Court Decides ? Which Law Applies ? Quel tribunal décide ? Quel droit s'applique ?, Kluwer Law International, Law and Electronic Commerce, vol. 5, 1998.

BORE (L.)
La défense des intérêts collectifs par les associations devant les juridictions administratives et judiciaires, (préf. Geneviève VINEY), tome 278, L.G.D.J., coll. *Bibl. dr. privé*, 1997.

BOUREL (P.)
Les conflits de lois en matière d'obligations extra-contractuelles, (sous la dir. d'Henry SOLUS), (préf. Yvon LOUSSOUARN), tome XXII, L.G.D.J., coll. *Bibl. dr. privé*, 1961.

BOUTONNET (M.)
Le principe de précaution en droit de la responsabilité civile, tome 444, L.G.D.J., 2005.

CACHARD (O.)
La régulation internationale du marché électronique, (préf. Philippe FOUCHARD), tome 365, L.G.D.J., coll. *Bibliothèque de Droit Privé*, 2002.

CARVAL (S.)
La responsabilité dans sa fonction de peine privée, (préf. VINEY), tome 250, L.G.D.J., coll. *Bibl. dr. privé*, 1995.

CHAMPY (G.)
La fraude informatique, (préf. Gaëtan DI MARINO et avant-propos Jacques GODFRAIN), P.U.A.M., 1992.

CHARDIN (N.)
Le contrat de consommation de crédit et l'autonomie de la volonté, (préf. J.-L. AUBERT), L.G.D.J., coll. *Bibl. dr. privé*¸ 1998.

CHEN (C-S), FILIPE (J.) et al.
Enterprise Information Systems VII, Springer, 2006

CNIL
Dix ans d'informatique et libertés, Economica, 1988.

CONSEIL D'ÉTAT
- *Les autorités administratives indépendantes*, Doc. fr., coll. *Études et Documents*, n° 52, 2001.
- *La révision de lois de bioéthique*, Doc fr., 2009.

COULON (J.-M.)
La dépénalisation de la vie des affaires, Doc. fr., coll. *Rapports officiels*, 2008.

COUR DE CASSATION
L'innovation technologique, Rapport annuel, 2005, Doc. fr., 2006.

COUTANT-LAPALUS (C.)
Le principe de la réparation intégrale en droit privé, (préf. Frédéric POLLAUD-DULIAN), P.U.A.M., 2002.

CROZE (H.), MORAL (C.) et FRADIN (O.)
Procédure civile, Litec, coll. *Objectif Droit cours*, 2008.

DEJEAN DE LA BATIE (N.)

Appréciation in abstracto et in concreto en droit civil français (préf. Henri MAZEAUD), L.G.D.J., 1965.

DELAHAIE (H.) ET PAOLETTI (F.)
Informatique et libertés, La Découverte, coll. *Repères*, Paris, 1987.

DEVEZE (J.)
Atteintes aux systèmes de traitement automatisé de données, J.-Cl. Pénal Code, Art. 323-1 à 323-7, fasc. unique, 1997.

FENOLL-TROUSSEAU (M.-P.) ET HAAS (G.)
Protection des données à caractère personnel – Vie privée et communication électronique, J.-Cl. Communication, Fasc. 4735, 2005.

FERAL-SCHUHL (C.)
Cyberdroit : Le droit à l'épreuve de l'internet, 6e éd., *Dalloz*, coll. *Praxis Dalloz*, 2010.

FILIPPONE (C.)
La contractualisation des droits de la personnalité, thèse sous la dir. de Philippe DELEBECQUE, Paris I, 2001.

FOURNIER (S.)
Pratiques commerciales trompeuses, J.-Cl. Lois pénales spéciales, Fasc. 20, 2008.

FRAYSSINET (J.)
- *Atteintes aux droits de la personne résultant des fichiers ou des traitements informatiques, J.-Cl. Pénal Code, Art. 226-16 à 226-24,* Fasc. 20, 2005.
- *Informatique, fichiers et libertés* (préf. Jacques FAUVET), Litec, 1992.

GANOT (J.)
La réparation du préjudice moral, Imprimerie Edoneur, Rennes, 1924.

GASSIN (R.)
- *Informatique (fraude informatique), Répert. pénal, Dalloz,* oct. 1995.

GOLDIE-GENICON (C.)
Contribution à l'étude des rapports entre le droit commun et le droit spécial des contrats, (préf. Yves LEQUETTE), tome 509, LGDJ, coll. *Bibl. dr. privé*, 2009.

GUEGAN-LECUYER (A.)
Dommages de masse et responsabilité civile, (préf. Patrice JOURDAIN, avant-propos Geneviève VINEY), tome 472, L.G.D.J., coll. *Bibl. dr. privé*, 2006.

GUTMANN (D.)
Le sentiment d'identité – Étude de droit des personnes et de la famille (préf. François TERRE), tome 327, L.G.D.J., coll. *Bibl. dr. privé*, 2000.

HALA (K.)
L'internaute et son droit à être laissé tranquille, sous la dir. de Jean FRAYSSINET, Mémoire DEA, Montpellier, 2003.

HEUZE (V.)
« La vente internationale de marchandises : droit uniforme », (sous la dir. de Jacques GHESTIN), L.G.D.J., coll. *Traité des contrats*, 2000.

ITEANU (O.)
L'identité numérique en question, Eyrolles, 2008.

JAULT (A.)
La notion de peine privée, (sous la dir. de François CHABAS), tome 442, L.G.D.J., coll. *Bibl. dr. privé,* 2005.

JOURDAIN (P.)
- Droit à réparation : Responsabilité fondée sur la faute. – Notion de faute : contenu commun à toutes les fautes, J.-Cl. Civil Code, Fasc. 120-10, 2006.
- Droit à réparation : Lien de causalité. – Détermination des causes du dommage, J.-Cl. Civil Code – Art. 1382 à 1386, Fasc. 160, 2005.

KAYSER (P.)
- La protection de la vie privée par le droit : Protection du secret de la vie privée, (préf. Henri MAZEAUD), 3e éd., Économica- P.U.A.M., 1995.

KNOPPERS (B. M.) et LABERGE (C. M.)
La Génétique humaine, de l'information à l'informatisation, éd. Litec/Thémis, 1992.

LARDEUX (G.)
Sources extra-contractuelles des obligations – Détermination de la loi applicable, J.-Cl. Droit international, Fasc. 553-1, 2008.

LE CLAINCHE (J.)
L'adaptation du droit des données à caractère personnel aux communications électroniques, sous la dir. de Nathalie MALLET-POUJOL et Jean FRAYSSINET, Montpellier 1, 2008.

LE GALLOU (C.)
La notion d'indemnité en droit privé, (préf. Alain SERIAUX), L.G.D.J., coll. *Bibl. dr. privé,* 2007.

LEPAGE (A.)
Libertés et droits fondamentaux à l'épreuve de l'internet : Droits de l'internaute, liberté d'expression sur l'internet, responsabilité, Litec, 2003.

LESAULNIER (F.)
L'information nominative, thèse sous la dir. de Pierre Catala, Paris II, 2005.

LOISEAU (G.)
Le nom objet d'un contrat (préf. Jacques GHESTIN), tome 274, L.G.D.J., coll. *Bibl. dr. privé,* 1997.

LOUSSOUARN (Y.)
« La règle de conflit est-elle une règle neutre ? », *Trav. Com. fr. DIP* 1980-1981, tome 2.

LUCAS (A.)
Le droit de l'informatique, P.U.F, coll. *Thémis Droit,* Paris, 1987.

LUCAS (A.), DEVEZE (J.) ET FRAYSSINET (J.)
Droit de l'informatique et de l'internet, P.U.F, coll. *Thémis Droit privé,* Paris, 2001.

MACKAAY (E.)

Nouvelles Technologies et propriété : actes du colloque tenu à la faculté de droit de l'Université de Montréal, les 9 et 10 novembre 1989, Thémis, Montréal, 1991.

MAITRE (G.)
La responsabilité à l'épreuve de l'analyse économique du droit, L.G.D.J., 2005.

MUIR-WATT (H.)
Domicile et résidence dans les rapports internationaux, J.-Cl.Civil Code, Art. 102 à 111, Fasc. unique, 2008.

NUYTS (A.)
L'exception de Forum non conveniens : Étude de droit international privé comparé, Bruylant/L.G.D.J., 2003.

- *Approches européenne et américaine de la liberté d'expression dans la société de l'information, J.-Cl. Communication*, Fasc. 1250, 2010.

PESKINE (E.)
Réseaux d'entreprises et du droit du travail, (préf. Antoine LYON-CAEN), LGDJ, coll. *Bibl. dr. social*, tome 45, 2008.

PIN (X.)
Droit pénal général, 3e éd., Dalloz, coll. *Cours*, 2009.

PRADEL (J.)
Droit pénal général, 17e éd., Cujas, coll. *Manuels*, 2008.

PRADEL (X.)
Le préjudice dans le droit civil de la responsabilité, tome 415, L.G.D.J., coll. *Bibl. dr. privé*, 1995.

RADE (C.)
Droit du travail et responsabilité civile, (préf. Jean HAUSER), L.G.D.J., coll. *Bibl. dr. privé*, tome 282, 1997.

RANO (L.-X.)
La force du droit à l'oubli, sous la dir. de Jean Frayssinet, Mémoire DEA Montpellier, 2004.

RASSAT (M.-L.)
- *Droit pénal spécial : Infractions des et contre les personnes*, 5e éd., Dalloz, coll. *Précis*, 2006.
- *Escroquerie, J-Cl. Pénal Code, Art. 313-1 à 313-3*, Fasc. 20, 2009.

RAYMOND (G.)
- *Publicité : Règles générales, J.- Cl. Commercial*, Fasc. 930, 2002.
- *Présentation de la loi n° 2008-3 du 3 janvier 2008 pour le développement de la concurrence au service des consommateurs, J.-Cl. Conc.-Conso.*, Fasc. 10 – Actualités, 2008.

RETIF (S.)
Droit à réparation : Conditions de la responsabilité délictuelle. – Le dommage. – Caractères du dommage réparable, J.-Cl. Civil Code, Art. 1283 à 1286, Fasc. 101, 2005.

REVERDY (P.-M.)

La matière pénale à l'épreuve des nouvelles technologies, thèse sous la dir. de Corinne MASCALA, Toulouse 1, 5 décembre 2005.

ROGERS (M.) et PEPPERS(D.)
Le One to One : valorisez votre capital client, Les Éditions d'Organisation, coll. *Pratique du marketing direct*, Paris, 1997.

SAINTOURENS (B.)
Essai sur la méthode législative : droit commun et droit spécial, thèse sous la dir. de Jean DERRUPE, Bordeaux I, 1986.

SMADJA (D.)
Bioéthique : aux sources des controverses sur l'embryon, (préf. Jean-Marie DONEGANI), Dalloz, coll. *Nouvelle Bibliothèque de thèses*, 2009.

STARCK (B.)
Essai d'une théorie générale de la responsabilité considérée en sa double fonction de garantie et de peine, thèse sous la dir. de Maurice PICARD, Paris, éd. Rostein, 1947.

TRIBES (R.)
Fondement et caractères de la réparation du préjudice moral, Imprimerie du Palais, Nice, 1932.

TRUDEL (P.) (sous la dir.)
Droit du cyberespace, Thémis, 1997.

VELU (J.)
Le droit au respect de la vie privée : Conférences données à la faculté de droit de Namur, Chaire René Cassin, (préf. René CASSIN), Presses Universitaires de Namur, coll. *Travaux de la Faculté de droit de Namur*, Namur et Bruxelles, 1974.

VITALIS (A.)
Informatique, Pouvoir et Libertés, (préf. Jacques ELLUL), 2e éd., Economica, coll. *Politique comparée*, Paris, 1988.

ARTICLES, COURS ET CHRONIQUES

- A -

AGGARWAL (R. K.) et WU (G.)
" Stock market manipulations", 79 *Journal of Business* 1915 (2006).

AL-FEDAGHI (S. S.)
" The " Right to be left alone " and Private Information " *in* Chin-Sheng CHEN, Joaquim FILIPE et al., *Enterprise Information Systems VII*, Springer, 2006, p. 157 et s.

ALONGI (E.)
Note, " Has the U.S. Canned Spam? ", 46 *Ariz. L. Rev.* 263 (2004).

ALTERMAN (H.) et BLOCH (A.)
« La fraude informatique », *Gaz. Pal.* 3 sept. 1988, 2, doctr., p. 530 et s.

AMBROISE-CASTEROT (.)
« Les nouvelles pratiques commerciales déloyales après la loi LME du 4 août 2008 », *AJ pénal* 2009, p. 22 et s.

ANCEL (M.-A.)
- « Un an de droit international privé du commerce électronique », *Comm. Com. électr.* janv. 2007, n°1, p. 1 ; janv. 2008 ; janv. 2009, pp. 17-22.
- « La contrefaçon de marque sur un site Web : Quelle compétence intracommunautaire par les tribunaux français ? », *in Droit et technique – Études à la mémoire du professeur Xavier Linant de Bellefonds*, *op. cit.*, p. 1 et s.

ANCEL (P.)
- « La protection des données personnelles : Aspects de droit privé français », *RIDC* 1987-3, p. 609 et s.
- « Les rapports de la responsabilité contractuelle et la responsabilité extra-contractuelle : Présentation des solutions de l'avant-projete, *RDC* 2007, p. 19 et s.

ARORA (V.)
Note, " The CAN-SPAM Act : An Inadequate Attempt to Deal with a Growing Problem ", 39 *Colum J.L. & Soc. Probs.* 299 (2006).

ATIAS (C.) et LINOTTE (D.)
« Le mythe de l'adaptation du droit aux faits », *D.* 1977, chron., p. 251 et s.

AUBERT (J.-L.)
« Quelques remarques sur l'obligation pour la victime de limiter les conséquences dommageables d'un fait générateur de responsabilité : À propos de l'article 1373 de l'avant-projet de réforme du droit des obligations », *in Études offertes à Geneviève VINEY*, L.G.D.J.-Lextenso, coll. *Les Mélanges*, 2008, spéc. p. 55 et s.

AUDIT (M.)
« L'interprétation autonome du droit international privé communautaire », *JDI* 2004, p. 789 et s.

AZZI (T.)
- « La loi du 29 octobre 2007 de lutte contre la contrefaçon : présentation générale », *D.* 2008, p. 708 et s.
- « Bruxelles I, Rome I, Rome II : regard sur la qualification en droit international privé communautaire », *D.* 2009, p. 1621 et s.

- B -

BALOUGH (R.)
" The Do-Not-Call Registry Model is Not the Answer to Spam ", 22 *J. Marshall J. of Comp. & Info. L.* 79 (2003).

BARBRY (É.)
« Spam et prospection commerciale : pas de vide juridique mais des modifications nécessaires », *Gaz. Pal*. 22 avr. 2004, n° 113, p. 27 et s.

BARBRY (É) ET POTTIER (I.)
« La CNIL et le rapport Olivennes luttent contre le téléchargement illicite, *Gaz. Pal.* 20-22 janv. 2008, n^{os} 20-22, p. 17 et s.

BARTELS (K. C.)
" Click Here to Buy the Next Microsoft " : The Penny Stock Rules, Online Microcap Fraud, and the Unwary Investor ", 75 *Indiana L.J.* 353 (2000).

BEGUIN (J.)
« Peut-on remédier à la complexité croissante du droit ? », *in Mélanges en l'honneur de Henry Blaise,* Economica, 1995, p. 1 et s.

BEHAR-TOUCHAIS (M.)
- « Rapport introductif », *in* « Existe-t-il un principe de proportionnalité en droit privé ? – Colloque Paris V, 20 mars 1998 », *LPA* 30 sept. 1998, n° 117, p. 3 et s.
- « L'amende civile est-elle un substitut satisfaisant à l'absence de dommages et intérêts punitifs ? », *LPA* 20 nov. 2002, n° 232, p. 36 et s.

BELLET (P.)
« L'élaboration d'une convention sur la reconnaissance des jugements dans le cadre du Marché Commun », *JDI* 1965, p. 833 et s.

BELLIA (P.L.)
" Defending Cyberproperty ", 79 *N.Y.U.L. Rev.* 2164 (2004).

BELLOIR (PH.)
« La répression pénale du " phishing " », *RLDI* janv. 2006, n° 349, p. 30 et s.

BELOT (F.)
- « Pour une reconnaissance de la notion de préjudice économique en droit français », *LPA* 28 déc. 2005, n° 258, p. 8 et s.
- « L'évaluation du préjudice économique », *D.* 2007, chron., p. 1681 et s.

BENICHOUX (J.-D.) et KHAYAT (Y.)
« La relativité de l'incompatibilité de la *class action* avec le système juridique français », *in* Daniel MAINGUY (sous la dir.), « L'introduction en droit français des class actions », *LPA* 22 déc. 2005, n° 254, p. 19 et s.

BENNETT (S. E.)
" *Canning Spam : CompuServe, Inc. v. Cyber Promotions, Inc. ",* 32 *U. Rich. L. Rev.* 545 (1998).

BENSOUSSAN (A.)
« Le " droit à l'oubli " sur Internet », *Gaz. Pal.* 6 févr. 2010, p. 3 et s.

BENYEKHLEF (K.)
« Les normes internationales de protection des données personnelles et l'autoroute de l'information », *in Le respect de la vie privée dans l'entreprise,* Thémis, 1996, Montréal, p. 66 et s.

BERAUDO (J.-P.)
« Le règlement (CE) du Conseil du 22 décembre 2000 concernant la compétence judiciaire, la reconnaissance et l'exécution des décisions en matière civile et commerciale », *JDI* 2001, p. 1033 et s.

BERGE (J.-S.)

« Droit d'auteur, conflits de lois et réseaux numériques : rétrospective et prospective », *Rev. Crit. DIP* juill.-sept. 2000, p. 357 et s.

BERLEUR (J.) et POULLET (Y.)
« Réguler Internet », *Études* 2002/11, tome 397, p.463 et s.

BERLIOZ (G.)
« Droit de la consommation et droit des contrats », *JCP* 1979, éd. G., I. 2954.

BERTREL (J.-P.)
« Liberté contractuelle et sociétés : Essai d'une théorie du " juste milieu " en droit des sociétés », *RTD com.* 1996, p. 595 et s.

BIOLAY (J.-J.)
« La nouvelle directive européenne relative aux pratiques déloyales : défense prioritaire du consommateur et pragmatisme », *Gaz. Pal*. 10 nov. 2005, n° 314, p. 3 et s.

BLANHUET(G.) ET LE GALL (J.- P.)
« La fiducie, une œuvre inachevée. Un appel à une réforme après la loi du 19 février 2007 », *JCP* 2007, éd. G., I. 169.

BLANKE (J.)
" Canned Spam : New State and Federal Legislation Attempts to Put a Lid on It ", 7 *Comp. L. Rev. & Tech. J.* 305 (2004).

BOCCARA (V.)
« Loi " informatique et libertés " : des sanctions fortes, des risques accrus », *LPA* 16 févr. 2005, n° 33, p. 3 et s.

BOLZE (A.)
« L'application de la loi étrangère par le juge français : le point de vue d'un processualiste », *D.* 2001, chron., p. 1818 et s.

BORCHERS (P. J.)
" New York Choice of Law : Weaving the Tangled Strands ", 57 *Alb. L. Rev*. 93 (1993-1994).

BORE (J.)
« L'indemnisation pour les chances perdues : une forme d'appréciation quantitative de la causalité d'un fait dommageable », *JCP* 1974, éd. G., I. 2620.

BORGHETTI (J.-S.)
- « La définition de la faute dans l'avant-projet de réforme du droit des obligations », *in* John CARTWRIGHT, Stefan VOGENAUER et Simon WHITTAKER (sous la dir.), *Regards comparatistes sur l'avant-projet de réforme du droit des obligations et de la prescription, op. cit.* , p. 295 et s.
- « Les intérêts protégés et l'étendue des préjudices réparables en droit de la responsabilité civile extra-contractuelle », *in Liber Amicorum, Études offertes à Geneviève VINEY, op. cit.*, p. 145 et s.

BORYSEWICZ (M.)
« Les règles protectrices du consommateur et le droit commun des contrats : Réflexions à propos de la loi n° 78-23 du 10 janvier 1978 sur la protection de l'information des consommateurs de produits et de services », *in Études offertes à Pierre KAYSER, op. cit.*, p. 91 et s.

BOSKOVIC (O.)
« L'autonomie de la volonté dans le règlement Rome II », *D.* 2009, chron., p. 1639 et s.

BOUCOURECHLIEV (J.)
« L'informatique face à la complexification du droit : facteur positif, négatif … ou pervers », *in Droit et informatique : L'hermine et la puce, op. cit.*, spéc. p. 41 et s.

BOURTHOUMIEUX (J.)
« Dommages punitifs », *RGDA* 1996, p. 861 et s.

BOYER (J.)
« La révolution d'internet », *LPA* 10 nov. 1999, n° 224, p. 11 et s.

BRIERE (C.)
« Le règlement (CE) n° 864/2007 du 11 juillet 2007 sur la loi applicable aux obligations non contractuelles (" Rome II "), *JDI* 2008, doctr., p. 31 et s.

BRUGUIERE (J.- M.)
- « " Deux ou trois choses… " que nous savons de la LCEN », *Contrats conc. conso.* déc. 2004, Étude 19.
- « La protection du cyber-consommateur dans la loi pour la confiance dans l'économie numérique », *RLDI* janv. 2005, n° 44, p. 59 et s.

BRUN (P.)
« Rapport introductif », *in* « La responsabilité civile à l'aube du XXI^e^ siècle : Bilan prospectif – colloque Chambéry, 7 et 8 déc. 2000 », *Resp. civ. assur.* juin 2001, n° 6 bis, *Resp. civ. assur.* juin 2001, n° 6 bis, p. 1 et s.

BRUNEAU (C.)
« Les règles européennes de compétence en matière civile et commerciale : Règl. Cons. CE n° 44/2001, 22 déc. 2000 », *JCP* 2001, éd. G, I. 304.

BURK (D. L.)
" The Trouble with Trespass ", 4 *J. Small & Emerging Bus L.* 27 (2000).

BURNSTEIN (M.)
« A Global Network in a Compartmentalised Legal Environment », *in* Katharina BOELE-WOELKI et Catherine KESSEDJIAN, *Internet Which Court Decides ? Which Law Applies ? Quel tribunal décide ? Quel droit s'applique ?, op. cit.*, p. 23 et s.

- C -

CABALLERO (F.)
« Plaidons par Procureur ! : De l'archaïsme procédural à l'action de groupe », *RTD civ.* 1985, p. 247 et s.

CABRILLAC (S.)
« Pour l'introduction de la class action en droit français », *LPA* 18 août 2006, n° 165, p. 4 et s.

CACHARD (O.)
« Définition du commerce électronique et loi applicable », *Comm. com. électr.* sept. 2004, Étude 31, p. 53 et s.

CADIET (L.)
« La notion d'information génétique en droit français », *in* Bartha Maria KNOPPERS et Claude M. LABERGE, *La Génétique humaine, de l'information à l'informatisation, op. cit.*, p. 41 et s.

CALAIS-AULOY (J.)
- « Les ventes agressives », *D.* 1970, chron., p. 37 et s.
- « L'influence du droit de la consommation sur le droit civil des contrats », *RTD civ.* 1994, p. 239 et s.

CAMERLYNCK (G.-H.)
« L'autonomie du droit du travail : la prescription abrégée de la créance des salariés », *D.* 1956, chron., p. 23 et s.

CANNARSA (M.)
« La réforme des pratiques commerciales déloyales par la loi Chatel : le droit commun à la rencontre du droit de la consommation », *JCP* 2008, éd. G., I. 180.

CAPRIOLI (É.)
- « Le phishing saisi par le droit », *Comm. com. électr*. févr. 2006, comm. 37, p. 47 et s.
- « Commerce à distance sur l'Internet et protection des données à caractère », *Comm. com. électr*. févr. 2005, Étude 7, p. 24 et s.

CAPRIOLI (É.) ET AGOSTI (P.)
« La confiance dans l'économie numérique (Commentaires de certains aspects de la loi pour la confiance dans l'économie numérique) », *LPA* 3 juin 2005, n° 110, p. 4 et s.

CARROLL (M.)
" Garbage In: Emerging Media and Regulation of Unsolicited Commercial Solicitations ", 11 *Berkeley Tech. L.J.* 233 (1996).

CARVAL (S.)
« Vers l'introduction en droit français de dommages intérêts punitifs ? », *RDC* 2006, p. 822 et s.

CATALA (P.)
- « Ébauche d'une théorie juridique de l'information », *D.* 1984, chron. p. 97 et s.
- « Le marché de l'information (aspects juridiques) », *LPA* 16 oct. 1995, n°124, p. 5 et s.
- « Unité ou complexité », *in Droit et informatique : L'hermine et la puce, op. cit.*, p. 3 et s.

CAVERS (D. F.)
" A Critique of the Choice-of-Law Process ", 47 *Harv. L. Rev.* 172 (1933).

CAVERS (D. F.), CHEATHAM (E.), CURRIES (B.), et al.
" Comments on Babcock v. Jackson, A Recent Development in Conflit of Laws ", 63 *Colum. L. Rev.* (1963).

CHAFIOL-CHAUMONT (F.) ET BONNIER (A.)
« L'identification des " pirates du Web " à partir de leur adresse IP », *RLDI* mai 2009, n° 1625, p. 84 et s.

CHAGNY (M.)
« Une (r)évolution du droit français de la concurrence ? – À propos de la loi LME du 4 août 2008 », *JCP* 2008, éd. G., I. 196.

CHAMOUX (F.)
« La loi sur la fraude informatique : de nouvelles incriminations », *JCP* 1998, éd. G., I. 3321.

CHAMPY (G.)
« Essai de définition de la fraude informatique », *RRJ* 1988-3, p. 751 et s.

CHARLEMAGNE (P.)
« La complexification de la société doit-elle entraîner la complexification du droit ? », *in Droit et informatique : L'hermine et la puce*, *op. cit.*, p. 21 et s.

CHAZAL (J.-P.)
« Réflexions épistémologiques sur le droit commun et les droits spéciaux », *in Études du droit de la consommation, Liber Amicorum Jean CALAIS-AULOY*, *op. cit.*, p. 279 et s.

CNIL
- « Dispositif d'analyse du comportement des consommateurs : souriez, vous êtes filmés ! », 19 avr. 2010, disponible sur : http://www.cnil.fr/la-cnil/actu-cnil/article/article/dispositifs-danalyse-du-comportement-des-consommateurs-souriez-vous-etes-comptes-2/.
- « Internet sans trace, ça n'existe pas ! », actualités, 11 janv. 2010, disponible sur : http://www.cnil.fr/la-cnil/actu-cnil/article/article/internet-sans-trace-ca-nexiste-pas/.
- « La véritable portée du problème : la collecte des *e-mails* dans les espaces publics de l'Internet », *in* CNIL, *Le publipostage électronique et la protection des données personnelles*, 14 oct. 1999, rapport préc., spéc. pp. 19-20.
- « Le droit d'opposition », disponible sur : http://www.cnil.fr/vos-libertes/vos-droits/le-droit-dopposition/.
- « Les observations de la CNIL sur l'article 22 de la loi du 21 juin 2004 pour la confiance dans l'économie numérique », disponible sur : http://www.cnil.fr/es/dossiers/commerce-publicite-spam/halte-au-spam/letat-du-droit-en-france/les-observations-de-la-cnil-sur-larticle-22-de-la-loi-du-21-juin-2004-pour-la-confiance-dans-leconomie-numerique/.
- « Panorama des législations », 2 juin 2008, disponible sur : http://www.cnil.fr/fileadmin/documents/approfondir/dossier/international/panorama-legislation.pdf).
- « Pas de liberté sans droit à l'oubli dans la société numérique », 27 novembre 2009, disponible sur : http://www.cnil.fr/la-cnil/actu-cnil/article/article/pas-de-liberte-sans-droit-a-loubli-dans-la-societe-numerique/.
- « Pas de publicité via *Bluetooth* sans consentement préalable », 13 nov. 2008, disponible sur : http://www.cnil.fr/es/la-cnil/actu-cnil/article/article/pas-de-publicite-via-bluetooth-sans-consentement-prealable/?tx_ttnews[backPid]=91&cHash=dd9280c396.
« Position de la CNIL sur la prospection par courrier électronique dans le cadre professionnel », 2 mars 2005, disponible sur : http://www.cnil.fr/es/la-cnil/actu-cnil/article/article/position-de-la-cnil-sur-la-prospection-par-courrier-electronique-dans-le-cadre-professionnel/
- « Tableau récapitulatif, Quelle déclaration pour quel fichier », disponible sur : http://www.cnil.fr/fileadmin/documents/approfondir/dossier/collec/TB-formalites-CL-VD.pdf
- « Vous souhaitez supprimer vos données sur internet : ayez le réflexe « plainte en ligne » ! », actualité, 24 nov. 2010, disponible sur : http://www.cnil.fr/dossiers/conso-pub-spam/actualites/article/vous-souhaitez-supprimer-vos-donnees-personnelles-sur-internet-ayez-le-reflexe-plainte-en-l/).
- « Vos traces sur internet : ce n'est pas virtuel ! », disponible sur : http://www.cnil.fr/vos-libertes/vos-traces/.
- « Le droit de rectification », disponible sur : http://www.cnil.fr/vos-libertes/vos-droits/le-droit-de-rectification/.

COBLENCE (J.-M.)
- « Le statut de la publicité dans la LCEN », *Comm. com. électr.* sept. 2004, Étude 25, p. 28 et s.
- « Publicité sur le net », *Expertises* 1997, p. 259 et s.

CONTAMINE-RAYNAUD (M.)
Le secret de la vie privée, in Yvon LOUSSOUARN et Paul LAGARDE (sous la dir.), *L'information en droit privé. Travaux de la conférence d'agrégation,* L.G.D.J., coll. *Bibl. dr. privé,* 1978, spéc. p. 402 et s.

CONTE (P.)
« Brèves observations à propos de l'incrimination des pratiques commerciales agressives », *Dr. pénal* févr. 2008, Étude 3, p. 7 et s.

CORDIER (G.)
« Les tranferts de données personnelles vers des pays tiers : suivez l'exemple ! », *Comm. com. électr.* juill. 2008, prat. 7, p. 44 et s.

COSTAZ (C.)
« Le droit à l'oubli », *Gaz. Pal.* 27 juill. 1995, doctr., p. 961 et s.

COUR DE CASSATION
« L'innovation technologique appréhendée par le juge », *in L'innovation technologique,* Rapport annuel, 2005, Doc. fr., 2006, p. 59 et s.

CROZE (H.)
« L'apport du droit pénal à la théorie générale du droit de l'informatique (à propos de la loi n° 88-19 du 5 janvier 1988 sur la fraude informatique), *JCP* 1998, éd. G., I. 3333.

CURRIE (B.)
" Notes on Methods and Objectives in the Conflict of Law ", 1959 *Duke L. J.* 171 (1959).

CYRIL VER HULST (C.)
« Dommage immatériel : du préjudice résultant des pertes d'exploitation », *LPA* 3 déc. 2001, n° 240, p. 4 et s.

- D -

DAHL (B.)
" A Further Darkside to Unsolicited Commercial Email? An Assessment of Potential Employer Liability for *Spam* Email ", 22 *J. Marshall J. of Comp. & Info. L.* 179 (2003).

DAUTIEU (T.)
« Le nouveau régime juridique applicable à la prospection directe opérée par voie électronique (À propos du projet de loi relatif à la confiance dans l'économie numérique) », *Gaz. Pal*. 1er nov. 2003, n° 305, p. 8 et s.

D'AVOUT (L.)
« Que reste-t-il du principe de territorialité des faits juridiques ? (une mise en perspective du système Rome II), *D.* 2009, chron., p. 1629 et s.

D'AVOUT (L.) et AZZI (T.) (dossier présenté par)

« Le règlement n° 864/2007 du 11 juillet 2007 sur la loi applicable aux obligations non contractuelles, dit " Rome II " », *D.* 2009, dossier, p. 1619 et s.

DECOOPMAN (N.)
« Droit du marché et droit des obligations », *in Le renouvellement des sources du droit des obligations, op. cit.*, p. 141 et s.

DELMAS-MARTY (M.)
« Du bon usage du droit comparé », *in* Mireille DELMAS-MARTY, *Critique de l'intégration normative : L'apport du droit comparé à l'harmonisation des droits, op. cit*., p. 227 et s.

DESSEMONTET (F.)
« Internet, la propriété intellectuelle et le droit international privé », *Internet,* Which *Court Decides ? Which Law Applies ?, op. cit.*, p. 47 et s., spéc. p. 57.

DEVEZE (J.)
« Commentaire de la loi n° 88-19 du 5 janvier 1988 relative à la fraude informatique », *Lamy Droit de l'informatique,* 1987, mise à jour févr. 1988, p. 3 et s.

DUFLOT (F.)
« " Phishing " : les dessous de la contrefaçon », *RLDI* janv. 2006, n° 366, p. 54 et s.

DUFOUR (O.)
« Une méfiance grandissante à l'égard des nouvelles technologies », *LPA* 27 juillet 2000, n° 149, p. 3 et s.

DUPICHOT (P.)
« Opération fiducie sur le sol français », *JCP* 2007, éd. G., actu. n° 121, p. 5.

DUPUIS (M.)
« La Vie privée à l'épreuve de l'internet : quelques aspects nouveaux », *RJPF* 2001.

DREIFUSS-NETTER (F.)
« Droit de la concurrence et droit commun des obligations », *RTD civ*. 1990, p. 369 et s.

DREYER (E.)
« Un an de droit de la publicité », *Comm. com. électr*. juill.-août 2008, étude 7, p. 15 et s.

DROUARD (É.)
« À propos de la loi " économie numérique " et débat " *opt-in* "/" *opt-out* ", il n'est pas encore interdit de réfléchir », Expertises 2004, n° 277, pp. 16-17.

DROZ (G. A. L.) et GAUDEMET-TALLON (H.)
« La transformation de la Convention de Bruxelles du 27 septembre 1968 en règlement du Conseil concernant la compétence judiciaire, la reconnaissance et l'exécution des décisions en matière civile et commerciale, *Rev. crit. DIP oct.-déc.* 2001, p. 601 et s.

DUPEYROUX (J.-J.)
« Droit civil et droit du travail : l'impasse », *Dr. soc.* 1988, p. 371 et s.

- E -

ELHOUEISS (J.-L.)

« L'élément d'extranéité préalable en Droit international privé », *JDI* 2003, p. 9 et s.

ELKIN-KOREN (N.)
" Let the Crawlers Crawl : On Virtual Gatekeepers and the Right to Exclude Indexing ", 26 *U. Dayton L. Rev*. 179 (2001).

ENGEL (L.)
« Vers une nouvelle approche de la responsabilité : Le droit français face à la dérive américaine », *in Qui est responsable ? Qui est coupable ?, Esprit* juin 1993, p. 5 et s.

ESMEIN (P.)
« La commercialisation du dommage moral », *D.* 1954, chron., p. 113 et s.

EPSTEIN (R. A.)
" Intel v. Hamidi: The Role of Self-Help in Cyberspace? ", 1 *J. L . Econ. & Pol'y* 147 (2005).

- F -

FABRE-MAGNAN (M.)
« Propriété, patrimoine et lien social », *RTD civ.* 1997, p. 583 et s.

FALLON (M.) et MEEUSEN (J.)
« Le commerce électronique, la directive 2000/31/CE et le droit international privé », *Rev. crit. DIP* juill.-sept. 2002, p. 435 et s.

FASQUELLE (D.)
« L'existence de fautes lucratives en droit français », *in* colloque Paris 5 préc., *LPA* 20 nov. 2002, n° 232, p. 27 et s.

FASQUELLE (D.) et MESA (R.)
« La sanction de la concurrence déloyale et du parasitisme et le rapport Catala », *D.* 2005, chron., p. 2666 et s.

FAURE-ABBAD (M.)
« La présentation de l'inexécution contractuelle dans l'avant-projet Catala », *D.* 2007, chron., p. 165 et s.

FAUVARQUE-COSSON (B.)
« Le droit international privé classique à l'épreuve des réseaux», *in* Georges CHATILLON, *Le droit international de l'Internet, op. cit.*, p. 55 et s.

FENOLL-TROUSSEAU (M.-P.)
« Les moteurs de recherche : un piège pour les données à caractère personnel », *Comm. com. élect.* janv. 2006, Étude 3, p. 22 et s.

FENOUILLET (D.)
- « Une nouvelle directive pour lutter contre les pratiques commerciales déloyales, *RDC* 2005, p. 1059 et s.
- « La loi de modernisation de l'économie du 4 août 2008 et réforme du droit des pratiques commerciales déloyales », *RDC* 2009, p. 128 et s.

FISHER (M. A.)

« The Right to Spam? Regulating Electronic Junk Mail », 23 *Colum.- Vla J.L. & Arts* 363 (2000).

FLECHEUX (G.)
« La situation juridique en France : Le point de vue des professions juridiques », *in Le droit comparé aujourd'hui et demain, op. cit.*, spéc. p. 61 et s.

FOGO (C. E.)
" The Postman Always Rings 4,000 Times : New approaches to Curb Spam? ", 18 *J. Marshall J. of Comp. & Info. L.* 915 (2000).

FORD (R. A.)
" Preemption of State Spam Laws by the Federal CAN-SPAM Act ", 72 *U. Chi. L. Rev.* 355, disponible sur : http://www.spamlaws.com/state/summary.shtml.

FOREST (D.)
« Trente ans et des poussières. Retour sur les premiers pas de la CNIL », *RLDI* janv. 2008, n° 1159, p. 77 et s.

FOURNIER (S.)
« De la publicité fausse aux pratiques commerciales trompeuses », *Dr. pénal* févr. 2008, Étude 4, p. 13 et s., spéc. n° 2.

FOYER (J.)
« Rapport de synthèse », *in Les nouveaux moyens de reproduction, Trav. Ass. H. Capitant,* 1986, p. 17.

FRANCK (J.)
« Action de groupe : les initiatives européennes en droit interne et en droit communautaire », *in* « Les " class actions " devant le juge français : rêve ou cauchemar ? – Colloque Paris, 18 nov. 2004 », *LPA* 10 juin 2005, n° 115, p. 19 et s.

FRAYSSINET (J.)
- « La loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, *Rev. dr. publ.* juillet-août 1978, n° 94/2, p. 1094 et s.
- « La loi du 6 janvier 1978, Informatique, fichiers et libertés : Présentation pédagogique et synthétique », *RRJ* 1987-1, p. 191 et s.
- « La loi relative à l'Informatique, aux fichiers et aux libertés, modifiée par la loi du 6 août 2004 : continuité et/ou rupture ? », *RLDI* oct. 2005, n° 267, p. 50 et s.
- « La protection des données personnelles est-elle assurée sur l'internet ? » *in Le droit international de l'internet, op. cit.*, p. 435 et s.
- « La régulation du respect de la loi Informatique, fichiers et libertés par le droit pénal : une épée en bois », *Legicom* 2009/1, n° 42, p. 23 et s.
- « *La traçabilité des personnes sur l'internet* », *Dr. et patr.* mai 2001, spéc. n° 93, p.76 et s.
- « Le pseudo droit à l'oubli appliqué à la presse », *Légipresse* oct. 2010, p. 273 et s., spéc. p. 275.
- « Le transfert et la protection des données personnelles en provenance de l'Union europenne vers les États-Unis : l'accord dit « sphère de sécurité » (ou safe harbour) », *Comm. com. électr.* mars 2001, chron. 7, p. 10 et s.
- « Nouvelles technologies de l'information et de la communication et protection des libertés des consommateurs », *in* Marie-Christine PIATTI (sous la dir.), *Les libertés individuelles à l'épreuve des NTIC*, P.U.L., 2001.
- « Trente ans après, la Loi " Informatique et Libertés " se cherche encore », *RLDI* janv. 2008, n° 1157, p. 69 et s.

- « La traçabilité des personnes sur l'internet, une possible menace pour les droits et libertés », *in* Philippe PEDROT (sous la dir.), *Traçabilité et responsabilité*, Economica, 2003, p. 88 et s.

FRISON-ROCHE (M.-A.)
- « Les principes originels du droit de la concurrence déloyale et du parasitisme », *RJDA* 6/94, p. 483et s.
- « Les résistances mécaniques du système français à accueillir la *class action* : obstacles et compatibilités », *in* colloque Paris préc., *LPA* 10 juin 2005, n° 115, p. 22 et s.

- G -

GAILLARD (E.)
« La double nature du droit à l'image », *D.* 1984, chron., p. 161 et s.

GALLOUX (J.-C.)
« Non à l'embryon industriel. Le droit européen des brevets au secours de la bioéthique, *D.* 2009, p. 578 et s.

GARDE (A.) et HARAVON (M.)
« Pratiques commerciales déloyales : naissance d'un concept européen, *LPA* 27 juin 2006, n° 127, p. 9 et s.

GASSIN (R.)
- « La protection pénale d'une nouvelle " universalité de fait " en droit français : Les systèmes de traitement automatisé de données (Commentaire de la loi du 5 janvier 1988 relative à la fraude informatique »), *D.* 1989, actu. législ., p. 5 et s.
- « Lois spéciales et droit commun », *D.* 1961, chron., p. 91 et s.

GAUMONT-PRAT (H.)
« Génie génétique, et brevetabilité du vivant : De la science au droit », *in* Nicole M. LE DOUARIN (sous la dir.), *Science, éthique et droit,* (préf. Claude ALLEGRE, postface François TERRE), Odile Jacob, 2007, p. 229 et s.

GAUDEMET-TALLON (H.)
- « Droit international privé de la contrefaçon : aspects actuels », *D.* 2008, dossier, p. 735 et s.
- « La compétence internationale à l'épreuve du Nouveau Code de procédure civile : aménagement ou bouleversement ? », *Rev. crit. DIP* janv.-mars 1977, p. 1 et s.
- « Les régimes relatifs au refus d'exercer la compétence juridictionnelle en matière civile et commerciale : forum non conveniens, lis pendens », *RIDC* 1994, p. 423 et s.

GAUTIER (P.-Y.)
- « Du droit applicable dans le « village planétaire » au titre de l'usage immatériel des œuvres », *D.* 1996, p. 131 et s.
- « L'équivalence des supports électronique et papier au regard du contrat », *in Droit et technique – Études à la mémoire du professeur Xavier Linant de Bellefonds*, Litec – LexisNexis, coll. *Les Mélanges,* 2007, p. 195 et s.
- « Fonction normative de la responsabilité : Le contrefacteur peut être condamné à verser au créancier une indemnité contractuelle par équivalent », *D.* 2008, Dossier, p. 727 et s.

GAUVIN (C.)
« Les sanctions de droits de la personnalité : Une étude de droit civil », *Comm. com. électr.* mars 2004, p. 14 et s.

GAVANON (I.)
« La directive "Commerce électronique" : continuité ou nouveauté juridique ?, *Comm. com. électr*. déc. 2001, chron. 28, p. 10 et s.

GEISSLER (J.)
“ Whether 'Anti-Spam' Laws Violate The First Amendment ”, *J. Online L*. art. 8 (2001).

GEIST (M. A.)
« Is there a There There? Towards Greater Certainty for Internet Jurisdiction », 16 *Berkeley Tech. L.J.* 1345 (2002).

GINDIN (S. E.)
“ Lost and Found in Cyberspace : Informational Privacy in the Age of the Internet”, 32 *San Diego L. Rev*. 1153 (1997).

GOLA (R.)
« Usurpation de l’identité sur l’internet : aspects de droit pénal comparé », *RLDI* déc. 2009, n° 1839, p. 65 et s.

GOLDMAN (B.)
« Un Traité fédérateur : la Convention entre les États membre de la C.E.E. sur la reconnaissance et l’exécution des décisions en matière civile et commerciale, *RTD eur*. 1971, p. 1 et s.

GOLDMAN (É.)
“ Where’s the Beef? Dissecting *Spam*’s Purported Harms ”, 22 *J. Marshall J. of Comp. & Info. L.* 13 (2003).

GORLA (G.)
« Intérêts et problèmes de la comparaison entre le droit continental et la Common law », *RIDC* 1963, p. 5 et s.

GRAYDON (S.)
“ Much Ado About Spam: Unsolicited Advertising, the Internet and You ”, 32 *St. Mary’s L.J.* 77 (2000).

GROSSMAN (S.)
“ Keeping Unwanted Donkeys and Elephants Out of Your Inbox : The Case for Regulating Political Spam ”, 19 *Berkeley Tech. L.J.* 1533 (2004).

GRUBER (A.)
« Le système français de protection des données personnelles », *LPA* 4 mai 2007, n° 90, p. 4 et s.

GRYNBAUM (L.)
- « La directive " Commerce électronique " ou l’inquiétant retour à l’individualisme juridique », *Comm. com. électr*. juill/août 2001, chron. 18, p. 9 et s.
- « Loi " Confiance dans l'économie numérique " : une version définitive proche de la version originale de la Directive " commerce électronique " », *Comm. com. électr*. juin 2004, comm. 78, p. 38 et s.
- « Une illustration de la faute lucrative : le " piratage " de logiciels », *D.* 2006, p. 655 et s.

GUERCHOUN (F.) et PIEDELIEVRE (S.)

« Le règlement sur la loi applicable aux obligations non contractuelles (" Rome II ") », *Gaz. Pal.* 21-23 et 28-30 oct. 2007, p. 3107 et s.

GUILLERMIN (P.)
« Droit de la consommation : l'absence d'une véritable alternative à la voie pénale » *in* Dossier : « Quelle dépénalisation pour le droit des affaires », *AJ Pénal* 2008, n° 2, p. 73 et s.

GUINCHARD (S.)
« Une *class action* à la française ? », *D.* 2005, doctr., p. 2180 et s.

GUYON (Y.)
« Le droit des contrats à l'épreuve du droit des procédures collectives », *in Le contrat au début du XXI^e siècle, Études offertes à Jacques GHESTIN, op. cit.*, p. 405 et s.

- H -

HAERI (K.)
« Réflexions sur me rapport du groupe de travail sur la dépénalisation de la vie des affaires : et le droit pénal n'appartient plus jamais au justiciable », *in* « Dépénalisation de la vie des affaires », Dossier spécial, *Dr. pénal* mars 2008, p. 13 et s.

HASS (G.) ET DE TISSOT (O.)
- « Le paradoxe du "droit à l'oubli" », *Expertises* 2005, p. 104 et s.
- « Le publipostage non sollicité dans le collimateur de la justice », *Expertises* 2002, p. 183 et s.

HASSLER (T.)
« La crise d'identité des droits de la personnalité », *LPA* 7 déc. 2004, n° 244, p. 3 et s.

HAWLEY (A. E.)
Comment, " Taking Spam Out of Your Cyberspace Diet : Common Law Applied to Bulk Unsolicited Advertising Via Electronic Mail ", 66 *UMKC L. Rev*. 381 (1997).

HUET (J.)
- « Aspects juridiques du commerce électronique : approche internationale », *LPA* 26 sept. 1997, n° 116, p. 6 et s.
- « Droit, informatique et rationalité », *in Droit et informatique : L'hermine et la puce, op. cit.*, spéc. p. 82.
- « Le droit applicable dans les réseaux numériques », *JDI* 2002, p. 737 et s.
- « Le droit pénal international et Internet », *LPA* 10 nov. 1999, n° 224, p. 39 et s.
- « Observations sur la distinction entre les responsabilités contractuelle et délictuelle dans l'avant-projet de réforme du droit des obligations, *RDC* 2007, p. 31 et s.
- « Perte de chance : du plus ou moins classique », *RTD* civ. 1986, p. 117 et s.

HUGUENEY (L.)
« Le sort de la peine privée en France dans la première moitié du XX^e siècle », *in Le privé français au milieu du XX^e siècle, Études offertes au professeur RIPERT, op. cit.*, p. 249 et s.

HUILLIER (J.)
« Propriété intellectuelle : des dommages et intérêts punitifs pas si punitifs », *Gaz. Pal.* 5-7 juill. 2009, n° 188, p. 2270 et s.

HUNTER (D.)

" Cyberspace as Place and the Tragedy of the Digital Anticommons ", 91 *Cal. L. Rev*. 439 (2003).

- I -

IVAINER (T.)
Le pouvoir souverain du juge dans l'appréciation des indemnités réparatrices », *D.* 1972, chron., p. 3 et s.

- J -

JAHAN (G.)
« Personal Data Privacy and Security Act : combattre le détournement de données personnelles sur internet », *Gaz. Pal.* 20 oct. 2005, 2, doctr., p. 3269 et s.

JAUFFRET-SPINOSI (C.)
« Les dommages-intérêts punitifs dans les systèmes de droit étrangers », *in* colloque Paris 5 préc., *LPA* 20 nov. 2002, n° 232, p. 8 et s.

JEANTIN (M.)
« Droit des obligations et droit des sociétés », *in Mélanges Laurent BOYER, op. cit.*, p. 317 et s.

JOBARD-BACHELLIER (M.-N.) et BREMOND (V.)
« De l'utilité du droit de la responsabilité pour assurer l'équilibre des intérêts des contractants (à propos des rapports entre droit commun et droit du cautionnement), *RTD* com. 1999, p. 327 et s.

JOSSERAND (L.)
« Un ordre juridique nouveau », *D.H.* 1937, chron., p. 41 et s.

JOUGLEUX (P.)
« La négligence dans la protection d'un système de traitement automatisé d'informations », *Expertises* 2000, p. 220 et s.

JOURDAIN (P.)
- « Rapport introductif » *in* colloque Paris 5 préc., *LPA* 20 nov. 2002, n° 232, p. 3 et s.
- « Réflexion sur la notion de responsabilité contractuelle », *in Les métamorphoses de la responsabilité, 6e journée R. Savatier,* P.U.F., coll. *Publications de la Faculté de droit et de sciences sociales de Poitiers*, tome 32, 1998, spéc. p. 65 et s.

JUENGER (F. K.)
" Babcock v. Jackson Revisited : Judge Fuld's Contribution to American Conflict Law ", 56 *Alb. L. Rev.* 727 (1992-1993).

- K -

KADNER GRAZIANO (T.)
« Le nouveau droit international privé communautaire en matière de responsabilité extracontractuelle (règlement Rome II) », *Rev. crit. DIP* juill.-sept. 2008 p. 445 et s.

KAPITANIAK (B.) et THILLIET-PRETNAR (J.)
Le clonage et le droit, in Nicole M. LE DOUARIN (sous la dir.), *Science, Éthique et droit, op. cit.,* p. 319 et s.

KAUFMANN-KOHLER (G.)
« Internet et mondialisation de la communication », *in* Katharina BOELE-WOELKI et Catherine KESSEDJIAN, *Internet : Which Court Decides ? Which Law Applies ?, op. cit.*, p. 89 et s.

KELIN (S.-A.)
« State Regulation of Unsolicited Commercial E-Mail », 16 *Berkeley Tech. L.J.* 435 (2001).

KESSEDJIAN (C.)
Rapport de synthèse in Katharina BOELE-WOELKI et Catherine KESSEDJIAN, *Internet : Which Court Decides ? Which Law Applies ?, op. cit.,* p. 143 et s.

KORZENIK (D.)
« La protection des droits de la personnalité aux États-Unis et en Grande-Bretagne : aspects de droit comparé », *in Les nouvelles frontières de la vie privée, Legicom* n° 43, 2009/2, p. 51 et s.

KOZINSKI (A.) & BANNER (S.)
"Who's Afraid of Commercial Speech? ", 76 *Va. L. Rev*. 627 (1990).

KRONKE (H.)
« Applicable Law in Torts and Contracts in Cyberspace » *in* Katharina BOELE-WOELKI et Catherine KESSEDJIAN, *Internet : Which Court Decides ? Which Law Applies ?, op. cit.,* spéc. p. 65 et s.

- L -

LAFOND (P.-C.)
« Le recours collectif et le juge Québécois : De l'inquiétude à la sérénité », *in* colloque Paris préc., *LPA* 10 juin 2005, n° 115, p. 11 et s.

LAGARDE (X.)
« Observations sur le volet consommation de la loi de modernisation de l'économie », *LPA* 23 févr. 2009, n° 38, p. 3 et s.

LAGHMANI (S.)
« Le droit international face aux nouvelles technologies, rapport introductif », *in* Rafâa BEN ACHOUR et Slim LAGHMANI, *Le droit international face aux nouvelles technologies, op. cit*.

LAPOYADE-DESCHAMPS (C.)
« La réparation du préjudice économique pur en droit français », *RIDC* 1998/2, p. 367 et s.
« Quelle(s) responsabilité(s) ? », *in* colloque Chambéry préc., *Resp. civ. assur*. juin 2001, n° 6 bis, p. 62 et s.

LARIOS (M. E.)
" E-Publius Unum: Anonymous Speech Rights Online ", 37 *Rutgers Law Record* 36 (2010).

LAROCHE-GISSEROT (F.)
« Les *class actions* américaines », *in* colloque Paris préc., *LPA* 10 juin 2005, n° 115, p. 7 et s.

LARROUMET (C.)
« Pour la responsabilité contractuelle », *in Le droit privé français à la fin du XX^e siècle, Études offertes à Pierre CATALA*¸. *op. cit.*, p. 543 et s.

LASSERRE CAPDEVILLE (J.)
« La substitution du délit de pratiques commerciales trompeuses au délit de publicité fausse ou de nature à induire en erreur », *LPA* 21 nov. 2008, n° 234, p. 8 et s.

LASTOWSKA (G.)
" Decoding Cyberproperty ", 40 *Ind. L. Rev.* 23 (2006).

LAUBADERE DE (A.)
« Loi relative à l'informatique, aux fichiers et aux libertés », *AJDA* mars 1978, n° 3, p. 146 et s.

LE (C.)
Note, " How Have Internet Service Providers Beat Spammers? ", 5 *Rich. J.L. & Tech. 9* (1998).

LEBRETON (G.)
« Y-t-il un progrès du droit, *D.* 1991, chron., p. 99 et s.

LECLERCQ (P.)
- « La CNIL, garante de la finalité, de la loyauté et de la sécurité des données personnelles » *in Les libertés individuelles à l'épreuve des NTIC*, P.U.L., 2001, p. 111 et s.
- « Loi du 6 août 2004. Transferts internationaux de données personnelles », *Comm. com. électr.* févr. 2005, Étude 8, p. 29 et s.
- « Un an d'application de la législation " informatique et libertés " », *Comm. com. électr.* juin 2006, chron. 6, p. 17 et s. ; *Comm. com. électr.* oct. 2007, chron. 9, p. 27 et s.

LECOMTE (F.) ET LEMAITRE (M.-H.)
« Inconnue juridique à cette adresse (IP) ou les affres du débat autour de la qualification de donnée à caractère personnel de l'adresse IP », *Expertises* 2008, p. 174 et s.

LEDIEU (M.- A.)
« Les transferts internationaux de données à la française », *Comm. com. électr*. janv. 2006, Étude 2, p. 17 et s.

LEGEAIS (D.)
« Le Code la consommation siège d'un nouveau droit commun du cautionnement : Commentaires des dispositions relatives au cautionnement introduites par les loi du 1er août 2003 relatives à l'initiative économique et sur la ville », *JCP* 2003, éd. E., 1433, p. 1610 et s.

LEGIER (G.)
« Le règlement " Rome II " sur la loi applicable aux obligations non contractuelles », *JCP* 2007, éd. G., I. 207.

LEPAGE (A.)
- « Internet : un nouvel espace de délinquance », *AJ Pénal* juin 2005, p. 217 et s., spéc. p. 217.
- « LCEN. Libertés sur Internet. Cybercriminalité », *Comm. com. électr*. sept. 2004, Étude 24, p. 24 ; *Droit pénal* déc. 2004, n° 12, Étude 24, p. 24 et s.
- « Loi du 6 août 2004. Réflexions de droit pénal sur la loi du 6 août 2004 relative à la protection des personnes à l'égard des traitements de données à caractère personnel », *Comm. com. électr.* févr. 2005, Étude 9, p. 33 et s.

- « Un an de droit pénal de la consommation (mars 2007 - avril 2008) », *Dr. pénal* mai 2008, chron. 4, p. 15 et s.
- « Un an de droit pénal de la consommation (avril 2008-avril 2009) », *Dr. pénal* mai 2009, chron. 5, p. 15 et s.
- « Un an de droit pénal de la consommation (avril 2009-avril 2010) », *Dr. pénal* mai 2010, chron. 4, p. 23 et s.

LEMOINE (P.)
« Commerce électronique, marketing et liberté » *in* Pierre TABATONI, *La protection de la vie privée dans la société de l'information*, *op. cit.*, p. 9 et s.

LETTERON (R.)
« Le droit à l'oubli », *RD publ.* 1996, p. 385 et s.

LETURMY (L.)
« La responsabilité délictuelle du contractant », *RTD civ* 1998, p. 839 et s.

LEVALLOIS-BARTH (C.) ET LICOPPE (C.)
« Le *Bluespam* et la CNIL », *Expertises* 2009, p. 217 et s.

LEVENEUR (L.)
- « Un peu de concurrence, beaucoup de droit de la consommation – À propos de la loi n° 2008-3 du 3 janvier 2008 », *JCP* 2008, éd. G., actu. 69.
- « Le Code civil, cadre normatif concurrencé », *in* Bernard SAINTOURENS, *Le Code civil, une leçon de légistique ?, op. cit.*, p. 123 et s.

LINANT DE BELLEFONDS (X.)
« De la LCI à la LCEN », *Comm. com. électr.* sept. 2004, Étude 22, p. 9 et s.

LIPOVETSKY (S.) ET YAYON-DAUVET (A.)
« Le devenir de la protection des données personnelles sur Internet », *Gaz. Pal.* 13 sept. 2001, 2, p. 2 et s.

LOQUIN (É.)
« L'approche juridique de la marchandisation », *in* Éric LOQUIN et Annie MARTIN (sous la dir.), *Droit et marchandisation*, Litec, Paris, 2010, p. 79 et s., spéc. n^{os} 36-37, p. 93.

LUCAS DE LEYSSAC (M.-P.)
« L'escroquerie par simple mensonge ? », *D.* 1981, chron., p. 17 et s.

LYON-CAEN (G.)
« Du rôle des principes généraux du droit civil en droit du travail (première approche) », *RTD civ.* 1974, p. 229 et s.

- M -

MAGEE (J.)
" The Law Regulating Unsolicited Commercial E-Mail : An International Perspective ", 19 *Santa Clara Computer & High Tech. L. J.* 333 (2003).

MAISL (H.)
- « État de la législation française et tendances de la jurisprudence relatives à la protection des données personnelles », *RIDC* 1978-3, p. 571 et s.

- « La maîtrise d'une interdépendance (commentaire de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés), *JCP* 1978, éd. G., I. 2891.

MAITROT DE LA MOTTE (A.)
« La réforme de loi informatique et libertés et le droit au respect de la vie privée », *AJDA* 2004, p. 2269 et s.

MALAURIE-VIGNAL (M.)
« Droit de la concurrence et droit des contrats », *D.* 1995, chron., p. 51 et s.

MALLET-POUJOL (N.)
« Appropriation de l'information : l'éternelle chimère », *D.* 1997, chron., p. 330.

MARCUS (J. A.)
Note, « Commercial Speech on the Internet : Spam and the First Amendment», 16 *Cardozo Arts & Ent. L.J.* 245 (1998).

MARIEZ (J.- S.)
« Un premier pas vers la mise en place d'un dispositif pertinent de lutte contre l'usurpation d'identité sur internet ? », *RLDI* nov. 2008, p. 65 et s.

MARINO (L.)
- « Les nouveaux territoires des droits de la personnalité », *Gaz. Pal*. 19 mai 2007, n° 139, p. 22.
- « Les contrats portant sur l'image des personnes », *Comm. com. électr*. mars 2003, chron. 7, p. 10 et s.

MARTINET (L.) et DE CHASTEL (A.)
« Du retour de l'action de groupe et du mythe de Sisyphe », *LPA* 10 mars 2009, n° 49, p. 6 et s.

MATSOPULOU (H.)
« L'oubli en droit pénal » *in Les Droits et le Droit, Mélanges dédiés à Bernard BOULOC*, *op. cit.*, p. 771 et s.

MATHEY (N.)
« Le commerce électronique dans la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique », *Contrats conc. conso.* oct. 2004, Étude 13, p. 7 et s.

MATTATIA (F.)
- « Internet face à la loi Informatiques et libertés : l'adresse IP est-elle une donnée à caractère personnel ? », *Gaz. Pal.* 15 janv. 2008, p. 9 et s.
- « CNIL et tribunaux : concurrence ou complémentarité dans la répression des infractions à la loi informatique et libertés », *Rev. sc. crim. et de dr. pénal comparé* avr.-juin 2009, p. 316 et s.

MAXWELL (W. J.), ZEGGANE (T.) et JACQUIER (S.)
« Publicité ciblée et protection du consommateur en France, en Europe et aux Etats-Unis », *Cont. conc. conso.* juin 2008, Étude 8, p. 18 et s.

MAYER (D.)
Note, " Attacking a Windmill : Why the CAN-SPAM Act Is a Futile Waste of Time and Money ", 31 *J. Legis*. 177 (2004).

MAZEAUD (D.)
« L'imbrication du droit commun et des droits spéciaux », *in* Geneviève PIGNARRE, *Forces subversives et forces créatrices en droit des obligations* : *Rétrospective et perspectives à l'heure du Bicentenaire du code civil, op. cit.*, p. 73 et s.

MEADEL (J.)
« Faut-il introduire la faute lucrative en droit français ? », *LPA* 17 avril 2007, n° 77, p. 6 et s.

MERRELL (R.C.)
Note, " Trespass to Chattels in the Age of the Internet ", 80 *Wash. U. L. Q*. 675 (2002).

MESA (R.)
« La consécration d'une responsabilité civile punitive : une solution au problème des fautes lucratives ? », *Gaz. Pal.* 21 nov. 2009, n° 325, p. 15 et s.

MIGUEL-CHESTERKINE (L.)
« Quelle protection pour l'internaute contre le publipostage informatique », *LPA* 23 févr. 2000, n° 38, p. 4.

MOLE (A.)
« Projet de loi informatique et libertés : le miroir à " deux faces " », *Gaz. Pal.* 16 oct. 2001, n° 289, p. 4 et s.

MOLE (A.) ET LEBON (H.)
« Publipostage électronique : entre certitudes et incertitudes », 1ère partie, *Gaz. Pal*. 18 avril 2002, n° 108, p. 29 et s.
« Publipostage électronique : entre certitudes et incertitudes », 2nde partie, *Gaz. Pal*. 13 juill. 2002, n° 194, p. 27 et s.

MOLFESSIS (N.)
« Le principe de proportionnalité et l'exécution du contrat » *LPA* 30 sept. 1998, n° 117, p. 21 et s.

MONSERIE (M. H)
« Aperçu sur les rapports récents de la confrontation du droit des procédures collectives et du droit des obligations », *in Prospectives du droit économique, Dialogues avec Michel JEANTIN, op. cit.*, p. 429 et s.

MOOREFIELD (G.)
Note, " *SPAM* – It's Not Just for Breakfast anymore : Federal Legislation and the Fight to Free the Internet From Unsolicited Commercial E-Mail ", 5 *B.U. J. Sci. & Tech. L*. 10 (1999).

MOSSOF (A.)
" Spam- Oy, What a nuisance ! ", 19 *Berkeley Tech. L.J*. 625 (2004).

MUIR WATT (H.)
« La fonction subversive du droit comparé », *RIDC* 2000, p. 503 et s., spéc. n° 18, p. 518.
« les principes généraux en droit international privé français », *JDI* 1997, p. 403 et s.

- N -

NATALSKI (F.)

« La loi " Informatique et libertés " n'est plus l'éternelle arlésienne », *RLDI* janv. 2008, n° 1158, p. 74 et s.

NERBONNE (S.)
« Le Groupe de l'article 29 est-il en mesure de s'imposer comme le régulateur des régulateurs par ses prises de position ? », *Legicom* 2009/1, n° 42, p. 37 et s.

NIBOYET (M.-L.)
« La révision de la Convention de Bruxelles du 27 septembre 1968 par le règlement CE du 22 décembre 2000 », *Gaz. Pal.* 10-12 juin 2001, doct., p. 943 et s.

NOURRISSAT (C.) et TREPPOZ (É.)
« Quelques observations sur l'avant-projet de proposition de règlement du Conseil sur la loi applicable aux obligations non contractuelles " Rome II " », *JDI* 2003, spéc. p. 7 et s.

- O -

OLLARD (R.)
« La distinction du dommage et du préjudice en droit pénal », *Rev. sc. crim.* juill.-sept. 2010, p. 561 et s.

O'ROURKE (M. A.)
" Property Rights and Competition on the Internet : In Search of an Appropriate Analogy ", 16 *Berkeley Tech. L.J.* 561 (2001).

- P -

PECH (L.)
« Approches européenne et américaine de la liberté d'expression dans la société de l'information, *Comm. com. électr.* juill.-août 2004, Étude 20, p. 13 et s.

PELISSIER (J.)
« Droit civil et contrat individuel de travail », *Dr. soc.* 1988, p. 387 et s.

PERE (D.) ET FOREST (D.)
« L'arsenal répressif du phishing », *D.* 2006, chron., p. 2666.

PERRAY (R.)
- « Adresse IP et données personnelles : un besoin de convergence d'interprétations entre juges, *Gaz. Pal.* 30 avr. 2009, p. 6 et s.
- « Quel avenir pour le pouvoir de sanction de la CNIL ? », *RLDI* janv. 2008, n° 1160, p. 82 et s.

PERREAU-SAUSSINE (L.)
« Les mal-aimés du règlement Rome II : les délits commis par la voie des médias », *D.* 2009, p. 1647 et s.

PETIT (F.)
« La mémoire en droit privé », *RRJ* 1997-1, p. 17 et s.

PIATTI (M.-C.)

« Avant-propos », *in* Marie-Christine PIATTI, *Les libertés individuelles à l'épreuve des NTIC*, *op. cit.*, p. 3.

PICARD (É.)
« L'état du droit comparé en France, en 1999 », *RIDC* 1999, p. 885 et s.

PICOD (Y.)
« Sanction du principe de proportionnalité en droit commun du cautionnement », *D.* 2004, chron., p. 204 et s.

PIEDELIEVRE (S.)
« Les dommages-intérêts punitifs : une solution d'avenir ? », *in* colloque Chambéry préc., *Resp. civ. assur*. juin 2001, n° 6 bis, étude 13, p. 68 et s.

PIETTE-COUDOL (T.)
« Les errances de la signature électronique ou comment résister à la convergence de la technique et du droit », *in Droit et technique – Études à la mémoire du professeur Xavier Linant de Bellefonds*, *op. cit.*, p. 395 et s.

PIZZIO (J.-P.)
« La protection des consommateurs par le droit commun des obligations », *RTD com.* 1998, p. 53 et s.

POLLAUD-DULIAN (F.)
- « Droit moral et droits de la personnalité », *JCP* 1994, éd. G., I. 3780.
- « Du droit commun au droit spécial – et retour », *in Aspects actuels du droit des affaires, Mélanges en l'honneur de Yves Guyon*, Dalloz, 2003, p. 925 et s.

POULLET (Y.)
- « Flux transfrontalières de données, vie privée et groupes d'entreprises », *RLDI* sept. 2005, n° 236, p. 47 et s.
- « Mieux sensibiliser les personnes concernées, les rendre acteurs de leur propre protection », *RLDI* mai 2005, n° 152, p. 47 et s.
- « Pour une justification des articles 25 et 26 de la directive européenne 95/46/CE en matière de flux transfrontalières et de protection des données », *Comm. com. électr*. décembre 2003, chron. 29, p. 9.
- « Le fondement du droit de la protection des données nominatives : " Propriété ou Libertés ", *in* Ejan MACKAAY, *Nouvelles Technologies et propriété : actes du colloque tenu à la faculté de droit de l'Université de Montréal*, *op. cit.*, p. 175 et s.

POUSSON (D.)
« L'identité informatisée » *in* Jacqueline POUSSON-PETIT (sous la dir. de), *L'identité de la personne humaine Etude de droit français et de droit comparé* , Bruylant, 2002, p. 371 et s.

PROUST (O.)
« État des lieux sur la proposition de loi du Sénat visant à modifier la loi " Informatique et libertés " », *RLDI* déc. 2009, n° 1823, p. 39 et s.

- Q -

QUILTER (L.)
Note, " The Continuing Expansion of Cyberspace Trespass to Chattels ", 17 *Berkeley Tech. L.J.* 421 (2002)).

- R -

RADE (C.)
« Responsabilité et solidarité : proposition pour nouvelle architecture », *D.* 2003, chron., p. 2247 et s.

RAYMOND (G.)
- « Incidences possibles de la transposition de la directive n° 2005/29/CE du 11 mai 2005 sur le droit français de la consommation », *Contrats, conc. conso*. janv. 2006, Étude 1, p. 5 et s.
- « Les modifications au droit de la consommation apportées par la loi n° 2008-3 du 3 janvier 2008 pour le développement de la concurrence au service des consommateurs », *Contrats, conc. conso*. mars 2008, Étude 3, p. 8 et s.

REMY (P.)
« La responsabilité contractuelle, histoire d'un faux concept », *RTD civ* 1997, p. 323 et s.

RICE (C.)
Comment, " The TCPA : A Justification for the Prohibition on Spam in 2002? ", 3 *N.C.J.L. & Tech* 375 (2002).

RIPERT (G.)
Le prix de la douleur », *D.* 1948, chron., p. 1 et s.

ROBINS (M.D.)
" *Electronic Trespass: An Old Theory in a New Context* ", 15 *Computer Lawayer* 1 (1998).

ROGERS (A. L.)
Note, " *Is There Judicial Recourse to Attack Spammers ?* ", 6 *Vand. J. Ent. L. & Prac*. 338 (2004).

ROUJOU DE BOUBEE (I.)
« Cryptographie : ses nécessités et ses dérives », *in* Marie-Christine PIATTI (sous la dir. de), *Les libertés individuelles à l'épreuve des NTIC*, P.U.L., 2001, spéc. p. 125 et s.).

RUELLAN (C.)
« La perte de chance en droit privé », *RRJ* 1999-3, p. 729 et s.

- S -

SAEDI (O.)
« Dommages-intérêts ou dommages et intérêts, celle-ci ou celle-là ; ou bien les deux », *LPA* 7 juin 2005, n° 12, p. 6 et s.

SAINT-ESTEBEN (R.)
« Pour ou contre les dommages et intérêts punitifs », *LPA* 20 janv. 2005, n° 14, p. 53 et s.

SAMORISKI (J. H.)
" Unsolicited Commercial E-mail, the Internet and the First Amendment : Another Free Speech Showdown in Cyberspace? ", 43 J. *Broad. & Elec. Media* 670 (1999).

SAVATIER (R.)
« Le Droit et l'accélération de l'Histoire », *D.* 1951,chron., p. 29 et s.

SAVAUX (É.)
« La fin de la responsabilité contractuelle », *RTD civ.* 1999, p. 1 et s.

SCHAUB (M.)
" Unsolicited Email : Does Europe Allow Spam ? The State of the Art of the European Legislation with Regard to Unsolicited Commercial Communications ", 18 *Computer L. & Sec. Rep*. 99 (2002).

SERNA (M.)
« L'image et le contrat : le contrat d'image », *Cont. conc. conso.* nov. 1998, chron. 12, p. 4 et s.

SERRA (Y.)
« Les fondements et le régime de l'obligation de non-concurrence », *RTD com.* 1998, p. 7 et s.

SILVERBRAND (I. J.)
" Commercialspeech.com : ACPA and the First Amendment ", 12 *UCLA J.L. & Tech.*, Issue 1, 1 (2008).

SIMON (G.)
La marchandisation du sportif : l'opération de transfert du footballeur », *in* Éric LOQUIN et Annie MARTIN (sous la dir.), *Droit et marchandisation, op. cit.*, p. 305 et s.

SIMON (M.)
Note, " The CAN-SPAM Act of 2003 : Is Congressional Regulation of Unsolicited Commercial E-Mail Constitutional? ", 4 *J. High Tech. L.* 85 (2004).

SIRINELLI (P.)
« L'adéquation entre le village virtuel et la création normative : Remise en cause du rôle de l'État ? » *in* Katharina BOELE-WOELKI et Catherine KESSEDJIAN, *Internet Which Court Decides ? Which Law Applies ?, op. cit*, p. 1 et s.

SLIM (H.)
« Approche comparative de la faute dans la responsabilité civile extra-contractuelle », *Resp. civ. assur.* juin 2003, chron. n° 18, p. 59 et s.

SORDINO (M.-C.)
« Flux et reflux du droit pénal au sein du droit des affaires (À propos de la « dépénalisation de la vie des affaires ») », *Gaz. Pal.* 24 mai 2008, n° 145, p. 2 et s.

SORKIN (D.)
- " Spam Legislation in the United States ", 22 *J. Marshall J. of Comp. & Info. L.* 3 (2003).
- " *Technical and Legal Approaches to Unsolicited Electronic Mail* ", 35 *U.S.F. L. Rev.* 325 (2001).
- " Unsolicited Commercial E-Mail and the Telephone Consumer Protection Act of 1991 ", 45 *Buffalo Law Review* 1001 (1997).

STEVENSON (R. L.)
" Plugging the " Phishing" Hole : Legislation versus Technology, 2005 *Duke L. & Tech. Rev. 6.*

SULLIVAN (J.) ET DE LEEUW (M.)
" Spam After CAN-SPAM : How Inconsistent Thinking Has Made a Hash Out of Unsolicited Commercial Email Policy ", 20 *Santa Clara Computer & High Tech L.J.* 887 (2004).

SUZSKIN (L.) ET DE GUILLENCHMIDT (M.)
« La qualification de l'adresse IP au centre de la lutte contre le téléchargement illicite sur les réseaux « peer to peer », *RLDI* déc. 2007, n° 1095, p. 6 et s.

SWEET (M.)
" Political E-Mail : Protected Speech or Unwelcome Spam? ", 2003 *Duke L. & Tech. Rev*. 1.

- T -

TABATONI (P.)
« Stratégies de la privacy aux États-Unis. La dynamique des systèmes de protection » *in* Pierre TABATONI (sous la dir.), *La protection de la vie privée dans la société de l'information, op. cit.*, spéc. p. 233.

TALLON (D.)
« L'inexécution du contrat : pour une autre présentation », *RTD civ*. 1994, p. 223et s.).

TEISSONIERE (G)
« La lutte contre le spamming : de la confiance en l'économie numérique à la méfiance envers ses acteurs », *Bull. Lamy*, avr. 2004, n° 168, p. 1 et s., spéc. p. 5.

TORRES (C.)
« Flux transfrontières de données : convention ou règles internes ? », *Gaz. Pal*. 20 juill. 2006, n° 201, p. 11 et s.

TOUCHENT (D.)
« La protection du consommateur contre les pratiques commerciales déloyales », *LPA* 2 août 2006, n° 153, p. 11 et s.

TREPPOZ (T.)
« La lex loci protectionis et l'article 8 du règlement Rome II », *D.* 2009, p. 1643 et s.

- V -

VAN OVERSTRAETEN (T.)
« Le règlement des litiges : tribunal compétent, loi applicable et modes alternatifs de règlement », *in* Étienne MONTERO, Jan DHONT, Daniel FESLER et al., *Le droit des affaires en évolution : Le contrat sans papier, op. cit.*, p. 237 et s.

VARET (V.)
« Le cadre juridique du *spam* : état des lieux », *Comm. com. électr*. sept. 2002, chron. 21, p. 14 et s.

VASSEUR-LAMBRY (F.)
L'identité de la personne humaine, *LPA* 6 mai 2004, n° 91, p. 5 et s.

VERBIEST (T.) ET WERY (É.)

« Commerce électronique par téléphone mobile (m-commerce) : un cadre juridique mal défini », *D.* 2004, chron., n° 41, p. 2.

VERON (P.)
- « Trente ans d'application de la Convention de Bruxelles à l'action en contrefaçon de brevet d'invention », *JDI* 2001, p. 805 et s.
- « Innovations apportées dans le contentieux de la propriété industrielle par le règlement 44/2001 du 22 décembre 2000 », *RDPI* mars 2001, n° 121, p. 4 et s.

VERON (P.) et ROUX-VAILLARD (S.)
« Les dommages-intérêts pour contrefaçon de brevet en droit américain », *RLDI* mars 2006, Étude 425, p. 67 et s.

VERPEAUX (M.)
« L'action de groupe est-elle soluble dans la Constitution ? », *D.* 2007, point de vue, pp. 258-259.

VINEY (G.)
- « L'appréciation du préjudice », *LPA* 19 mai 2005, n° 99, p. 89 et s.
- « Pour ou contre un " principe général " de responsabilité pour faute ? : Une question posée à propos de l'harmonisation des droits civils européens » *in Le droit privé français à la fin du XX^e siècle, Études offertes à Pierre CATALA, op. cit.*, p. 555 et s.
- « Rapport de synthèse » *in* « Faut-il moraliser le droit français de la réparation du dommage ? (À propos des dommages et intérêts punitifs et de l'obligation de minimiser son propre dommage) », colloque Paris 5, 21 mars 2002, *LPA* 20 nov. 2002, n° 232, p. 66 et s.

VIVANT (M.)
- « Cybermonde : Droit et de droits des réseaux », *JCP* 1996, éd. G., I. 396.
- « Le patronyme saisi par le patrimoine », *in Mélanges André Colomer*, *op. cit.*, p. 517 et s.
- « Les transferts internationaux de données dans la loi de 2004 », *RLDI* oct. 2005, n° 270, p. 64 et s.
- « Prendre la contrefaçon au sérieux », *D.* 2009, chron., p. 1839 et s.
- « Sciences et praxis », *D.* 1993, chron., p. 109 et s.

VIVANT (M.) et LE STANC (C.)
« Droit de l'informatique », *JCP* 1995, éd. E., I. 461.

- W -

WARREN (S. D.) et Louis D. BRANDEIS (L.)
« The Right to Privacy », *Harv. L. Rev.*, 193-220 (1890).

WEILL (A.)
Un cas épineux de compétence législative : le cas de la dissociation entre le fait générateur et le préjudice », *in Mélanges offerts à Jacques Maury, op. cit.*.

WEILL (P.- A.)
« État de la législation et tendances de la jurisprudence relatives à la protection des données personnelles en droit pénal français », *RID. comp*. 1987-3, p. 655 et s.

WENGLER (W.)
« L'évolution moderne du droit international privé et la prévisibilité du droit applicable », Rev. crit. *DIP* 1990, p. 657 et s.

WILHELM (C.) ET PENVEN (A.)
« La prospection commerciale par courrier électronique : le nouvel article L.121-20-5 du Code de la consommation », *Légipresse* oct. 2004, n° 215

- Y -

YANG (G.)
" CAN-SPAM: The First Step to No-Spam ", 4 *Chi-K. J. Intel. Prop.* 1 (2004).

- Z -

ZHANG (L.)
" CAN-SPAM Act : An Unsufficient Response to the Growing Spam Problem ", 20 *Berkeley Tech. L.J.* 301 (2005).

INDEX CHRONOLOGIQUE DE LA JURISPRUDENCE FRANÇAISE, COMMUNAUTAIRE ET ETRANGERE

1827 – 1960
- Cass. req., 15 nov. 1827, *S.* 1828, 1, p. 124.
- *Whitney v. California*, 274 *U.S.* 357, spéc. 373 (May 16, 1927).
- *Bridges v. California*, 314 *U.S.* 252 (Dec. 8, 1941).
- Cass. civ. 25 mai 1948, *Lautour*, *JCP* 1948, G., II. 4542, note M. Vasseur ; *D.* 1948, p. 357, note P. L. ; *Rev. crit. DIP* 1949, p. 89, note H. BATIFFOL ; *GAJFDIP*, 5e éd., *Dalloz*, 2006, n° 19, p. 164 et s. ; *S.* 1949. 1. 21, note Niboyet.
- Cass. civ., 9 mars 1949, *JCP* 1949, éd. G., II. 4826 ; *D.* 1949, p. 331 et s.
- CA Douai, 16 mars 1953, *D.* 1954, somm., p. 3.
- Cass. civ. 2e, 9 juill. 1954, *D.* 1954, jurispr., p. 627.
- Cass. civ. 2e, 28 oct. 1954, *Bull. civ.* II, n° 328 ; *RTD civ.* 1955, p. 324, spéc. n° 34, p. xxx, obs. H. et L. Mazeaud ; *JCP* 1955, éd. G., II. 8765, note R. Savatier.
- Cass. crim., 16 oct. 1957, *Bull. crim.* 1957, n° 636 ; *JCP* 1957, éd. G., IV. 166.
- Cass. civ. 1re, 19 oct. 1959, *Pelassa*, *D.* 1960, jurispr., p. 37 et s., note G. Holleraux ; *Rev. crit. DIP* avr.-juin 1960, p. 215 et s., note Y. Loussouarn ; *JDI* 1960, p. 486 et s., obs. J.-B. Sialelli.

1961
- *Roberts v. Permanente Corp.*, 188 *Cal. App. 2d*. 526, 10 *Cal. Rptr*. 519 (Ct. App. Jan. 26, 1961).
- Cass. crim., 15 févr. 1961, *D.* 1961, jurispr., p. 276.

1962
Cass. civ. 1re, 30 oct. 1962, *Scheffel*, *JDI* 1963, p. 1072 et s., obs. J.-B. Sialelli; *Rev. crit. DIP* janv.-mars 1963, p. 387 et s., note Ph. Francescakis ; *D.* 1963, jurispr., p. 109 et s., note G. Holleaux, *GAJFDIP*, n° 37, p. 319 et s.

1963

- Cass. civ. 2e , 1er avr. 1963, *D.* 1963, p. 453, note H. Molinier ; *JCP* 1963, II. 13408, note P. Esmein.
- Cass. civ. 2e, 18 déc. 1963, *Bull. civ.* II, n° 845.

1964
Cass. civ. 2e, 8 mai 1964, *JCP* 1965, éd. G., II. 14140, note P. Esmein ; *RTD civ.* 1965, n° 20, p. 137, obs. R. Rodière.

1965
Cass. civ. 2, 28 avr. 1965, *D.* 1965, p. 777 et s., note P. Esmein.

1966
- Cass. crim., 19 juill. 1966 , *JCP* 1966, éd. G., IV. 134.
- Cass. crim., 21 juill. 1966, pourvoi n° 66-90.465 ; *Bull. crim.*, n° 208.

1967
- Cass. crim. 14 mars 1967, pourvoi n° 66-92.369 ; *Bull. crim.* 1967, n° 102 ; *D.* 1967, somm., p. 50.
- Cass. civ. 1re, 30 mai 1967, *Kieger c/ Amigues*, *Rev. crit. DIP* oct.-déc. 1967, p. 728, note P. Bourel ; *JDI* 1967, p. 622 et s., note B. G. *; D.* 1967, jurispr., p. 629 et s., note P. Malaurie ; *JCP* 1968, éd. G., II. 15456, note A. Jack Mayer.
- CA Paris, 15 déc. 1967, *JCP* 1967, éd. G., II. 15107, note H.B. ; *RTD civ.* 1971, p. 114, obs. R. Nerson.

1968
- Cass. crim., 1er avr. 1968, pourvoi n° 67-92557 ; *Bull. crim.* 1968, n° 115 ; *JCP* 1968, éd. G., IV. 91.
- Cass. crim. 25 mars 1968, *D.* 1958, somm., p. 131.

1969
- Cass. crim., 6 févr. 1969, pourvoi n° 66-91594 ; *Bull. crim.* 1969, n° 65 ; *JCP* 1969, éd. G., II. 16116, note H. Guérin.
- Cass. civ. 2e, 23 avr. 1969, *Bull. civ.* II, n° 132 ; *D.* 1969, p. 562; *JCP* 1969, éd. G., II. 1596.
- Cass. civ. 1re, 16 juin 1969, *Bull. civ.* I, n° 184 ; *D.* 1969, p. 586 ; *JCP* 1970, éd. G., II. 16412, note R. Savatier.
- Cass. crim., 4 nov. 1969, *D.* 1970, p. 169.
- Cass. crim., 10 déc. 1969, pourvoi n° 67-91.046 ; *Bull. crim.* 1969, n° 335.

1970
- TGI Paris, 27 févr. 1970, *JCP* 1970, éd. G., II. 16293, note R. Lindon.
- *Rowan v. United States Post Office Dept.*, 397 *U.S.* 728 (May 4, 1970).
- Cass. crim., 10 déc. 1970, *Ministère Public et Mairie de la ville de Nice c/ Baraldini*, 1re espèce, *JCP* 1972, éd. *G.*, II. 17277, note R. Gassin.

1971
- Cass. civ. 2e, 15 déc. 1971, pourvoi n° 70-12603 ; *Bull. civ.* II, n° 345 ; *JCP* 1972, éd. G., IV, n° 30 ; *D.* 1972, somm., p. 96.
- Cass. crim., 21 déc. 1971, *D.* 1972, jurispr., p. 465, note J.-M. Rétant.

1972
- Cass. civ. 2e, 9 nov. 1972, *Bull. civ.* II, n° 276 ; *JCP* 1972, éd. G., IV. 294.
- CA Versailles, 4 févr. 2009, *D.* 2009, p. 819, obs. M. Boutonnet ; *JCP* 2009, éd. G., act. 83, obs. C. Bloch, et *idem.*, I. 248, spéc. n° 3, obs. Ph. Stoffel-Munck.

1973
- Cass. civ. 2e, 18 janv. 1973, *JCP* 1973, II. 17545, note M. A ; *RTD civ.* 1974, p. 159, obs. G. Durry.
- Cass. civ. 2e, 10 oct. 1973, pourvoi n° 72-12867 ; *Bull. civ.* II, n° 254.

1974

1975
CA Orléans, 23 oct. 1975, *JCP* 1977, éd. G., II. 18653, note Ph. Le Tourneau.

1976
- Cass. crim., 11 févr. 1976, pourvoi n° 75-91.806 ; *Bull. crim.*, n° 54, p. 128 ; *D.* 1976, p. 295, note Rapp. Dauvergne.
- Cass. civ. 1re, 1er juin 1976, *Luccantoni, JDI* 1977, p. 91, note B. Audit ; *D.* 1977, jurispr., p. 257 et s., note F. Monégier ; *JCP* 1979. éd. G., II. 19082, note F. Chabas.
- CJCE, 14 oct. 1976, *LTU c/ Eurocontrol*, aff. 29/76, *Rev. crit. DIP* 1977, p. 772, note G. Droz ; *JDI* 1977, chron., p. 707 et s., note A. Huet.
- CJCE, 30 nov. 1976, aff. 21/76, *Sté Bier et Fondation Rheinwater c. Sté Mines de potasse d'Alsace*, spéc. pts 24 et 25, *D.* 1977, jurispr., p. 613, note G. Droz ; *JDI* 1977, p. 728, obs. A. Huet ; *Rev. crit. DIP* 1977, p. 563, note P. Bourel.

1977
- CA Paris, 4 juill. 1977, *JCP* 1997, éd. G., II. 1978, note G. Flécheux.

1978
- Cass. crim., 23 mars 1978, pourvoi n° 77-92792 ; *Bull. crim.* 1978, n° 116 ; *D.* 1979, p. 319, note B. Bouloc ; *Rev. sc. crim.* 1979, p. 343 et s., obs. B. Bouzat.
lautour
- Cass. crim., 4 déc. 1978, pourvoi n° 77-92.400 ; *Juris-Data* n° 1978-799342 ; *Bull. crim.* 1978, n° 342 ; *Gaz. Pal.* 9 mai 1979, 1, p. 129.

1979
- Cass. com., 3 mai 1979, *Bull. civ.* IV, n° 137.
- TGI Paris, réf., 6 déc. 1979, *D.* 1980, jurispr. p. 150, note R. Lindon.

1980
- Cass. crim., 16 janv. 1980, pourvoi n° 79-91793, *Bull. crim.* 1980, n° 25 ; *D.* 1980, I.R., p. 409, obs. C. Larroumet ; *JCP* 1980, éd. G., IV. 124.
- *Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n of New York*, 447 *U.S.* 557, spéc. 561 (June 20, 1980).
- Cass. civ. 1re, 3 déc. 1980, *aff. Le pull-over rouge, D.* 1981, jurispr., p. 221, note B. Edelman.
- TGI Lyon, 17 déc. 1980, *Asvel Basket et Gilles et a. c/ Sté Anon et Lumière et Sté Anon-Euro-Advertising, D.* 1981, jurispr., p. 202, note R. Lindon et D. Amson.

1982
- TGI Paris, 12e ch. corr., 13 janv. 1982, *D.* 1982, I.R., pp. 501-502, obs. M. Vasseur ; *D.* 1985, I.R., p. 46, obs. J. Huet.
- Cass. civ. 2e, 4 févr. 1982, *inédit*, pourvoi n° 80-17139 ; *JCP* 1982, éd. G., II. 1984, note J.-F. Barbieri ; *Gaz. Pal.* 1983, pan., p. 355, note F. Chabas.
- TGI Paris, 13e ch. corr., 9 févr. 1982, *D.* 1982, IR, p. 502, note M. Vasseur.
- Cass. crim., 16 févr. 1982, pourvoi n° 81-92.263 ; *Bull. crim.* 1982, n° 54.
- CA Paris, 26 mai 1982, *Juris-Data* n° 1982-025335.
- Cass. crim., 9 juill. 1982, *inédit.*

- *Wilson et al. v. Interlake Steel Co*. et al., 185 *Cal. Rptr*. 280, 32 *Cal.3d.* 229 (Aug. 30, 1982).

1983
- Cass. civ. 1re, 8 févr. 1983, *Horn y Prado, JDI* 1984, p. 123 et s., note G. Légier.
- TGI Paris, 20 avril 1983, *JCP* 1985, éd. G., II. 20434, obs. R. Lindon.
- TGI Paris, 27 avr. 1983, 2e esp., *Rev. crit. DIP* oct.-déc. 1983, p. 670 et s., note H. Gaudemet-Tallon.
- Cass. civ. 2e, 6 juill. 1983, pourvoi n° 82-10581; *Bull. civ.* II, n° 143.
- Cass. civ. 2e, 9 nov. 1983, *Bull. civ.* II, n° 175 ; *JCP* 1985, éd. G., II. 20360, note Y. Chartier.

1984
- CA Paris, 1re ch., sect. A, 19 mars 1984, *Caroline de Monaco c/ Sté Burda Gmbh*, 1re esp., *D.* 1985, I.R., p. 179 et s., obs. B. Audit ; *Rev. crit. DIP* janv.-mars 1985, p. 141 et s., note H. Gaudemet-Tallon ; *Gaz. Pal.* 2-3 janv. 1985, nos 2-3, p. 7 et s., note J. Mauro.
- Cass. Ass. plén., 9 mai 1984, pourvois n° 80-93.031 (arrêt *Lemaire*) et 80-93481 (arrêt *Derguini*) ; *JCP* 1984, éd. G., II. 20256, note P. Jourdain ; *D.* 1984, p. 525 et s., concl. J. Cabannes, note F. Chabas ; *RTD civ.* 1984, p. 508 et s., obs. H. Huet.
- TGI Marseille, 6 juin 1984, *Izzo c/ Sté Seppim* (2e espèce), *D*. 1985, somm., p. 323 et s., obs. R. Lindon.
- Cass. civ. 1re, 16 oct. 1984, *JCP* 1984. IV. 357.

1985
- *Bradley v. Am. Smelting & Refining. Co.*, 104 Wn.2d 677, *P.2d* 782 (Wash. 1985).
- Cass. civ. 2e, 27 févr. 1985, *Bull. civ.* II, n° 52 ; *RTD* civ. 1986, p. 117, obs. J. Huet.
- Cass. com. 12 mars 1985, *Bordas*, pourvoi n° 84-17.163 ; *Rev. sociétés* 1985, p. 607, note G. Parleani ; *D.* 1985. jurispr., p. 471, note J. Ghestin ; *JCP* 1985, éd. G., II. 20400, concl. M. Montanier et note G. Bonet ; *Gaz. Pal*. 1985, 1, p. 246, note G. Le Tallec
- Cass. crim., 3 juin 1985, pourvoi n° 83-95.073, *Bull. crim.*, n° 211.
- Cass. civ. 1re, 19 nov. 1985, *Orliac, Bull. civ.* I, n° 306, p. 271 et s. ; *Rev. crit. DIP* 1986, p. 712 et s., note Y. Lequette ; *JDI* 1986, p. 719 et s., note A. Huet.

1986
- Cass. civ. 1re, 24 juin 1986, pourvoi n° 84-15215, *Bull. civ.* I, n° 178.
- Trib. Corr. de Versailles, 23 septembre 1986, *D.* 1987, jurispr., p. 552 et s., note J. Frayssinet.

1987
- Cass. crim., 16 mars 1987, pourvoi n° 86-92.932 ; *Bull. crim.*, n° 124, p. 346.
- TGI Paris, 25 mars 1987, *D*. 1988, somm. p. 198, obs. D. Amson.
- Cass. crim. 19 mai 1987, *Gaz. Pal.* 1988, 1, somm., p. 5.
- Cass. crim. 3 nov. 1987, pourvoi n° 87-83429, *Bull. civ*. 1987, n° 382.
- Cass. crim., 8 déc. 1987, pourvoi n° 85-92.404; *Bull. crim.*, n° 451, p. 1194 ; *RTD com.* 1988, p. 668, obs. J. Hémard et B. Bouloc ; *Rev. sc. crim.* oct.-déc. 1988, p. 808, obs. J.-Cl. Fourgoux.

1988
- CJCE, 5e ch., 27 sept. 1988, aff. 189/87, *Kalfelis, Rec. CJCE* 1988, p. 5565 et s. ; *Rev. crit. DIP.* janv.-mars 1989, p. 112 et s., note H. Gaudemet-Tallon ; *JDI* 1989, p. 457 et s., obs. A. Huet ; *D.* 1989, somm., p. 254 et s., note B. Audit.
- Cass. civ. 2e, 5 oct. 1988, *Gaz. Pal.* 1988, 2, pan., p. 270 ; *ibid.* 1989, 2, somm. p. 371, obs. F. Chabas.
- TGI Aix-en-Provence, 1re ch., 24 nov. 1988, *Brun c/ SA Expobat et a.*, *JCP* 1989, éd. G., II. 21329, obs. J. Henderycksen.
- TGI Rennes, 8 déc. 1988, *Expertises* 1989, n° 115, p 104 et s., note J. Frayssinet

1989
- Cass. civ. 2e, 8 févr. 1989, *RTD civ.* 1989, p. 556 et s., obs. P. Jourdain.
- Cass. civ. 1re, 7 juin 1989, *RTD* civ. 1992, p. 113 et s., obs. P. Jourdain.
- CA Versailles, 14 sept. 1989, *Jamet, Tesson et a. c/ consorts Girard*, *Gaz. Pal.* 1990, 1, somm. p. 123.
- Cass. com. 5 déc. 1989, pourvoi n° 87-15309, *Bull. civ.* IV, n° 307 ; *D.* 1990, I.R., p. 14.

1990
- CJCE, 11 janv. 1990, aff. C-220/88, *Sté Dumez c/ Hessische Landesbank*, spéc. pts 10 et 17, *Rec. CJCE*, I, p. 49 ; *Rev. Crit. DIP* avr.-juin 1990, p. 386 et s., note H. Gaudemet-Tallon ; *JDI* 1990, p. 497 et s., obs. A. Huet.
- Cass. 2e civ., 7 févr. 1990, *Juris-Data* n° 1990-700371, pourvoi n° 86-17023 ; *Bull. civ.* II, n° 21 ; *RTD civ.* 1990, p. 487 et s., obs. P. Jourdain.
- Cass. com., 27 févr. 1990, *Mazenod*, pourvoi n° 88-19.194 *; JCP* 1990, éd. G., II. 21545, note F. Pollaud-Dulian.
- Cass. crim., 28 févr. 1990, *RTD* civ. 1990, p. 670, obs. P. Jourdain.
- Cass. crim., 8 mars 1990, *Juris-Data* n° 1990-001311 ; *JCP* 1990, éd. G., II. 21542, note J.-H. Robert.
- Cass. civ. 2e, 4 juill. 1990, *Juris-Data n°* 1990-003025 ; *Resp. civ. et assur.* nov. 1990, spéc. n° 357, obs. H. Groutel ; *Gaz. Pal.* 1990, 2, pan., p. 233.
- Cass. crim., 4 oct. 1990 *; Bull. crim.* 1990, n° 331 ; *JCP* 1991, éd. G., IV. 8.
- Cass. civ. 1re, 20 nov. 1990, *Mme Monanges c/ Kern et a.*, pourvoi n° 89-12.580, *Bull. civ.* 1990, n° 256, *JCP* 1992, éd. G., II. 21908, note J. Ravanas ; *D.* 1991, chron., p. 176, n° 2, obs. A. Bénabant.

1991
- Cass. civ. 1re, 4 avr. 1991, pourvoi n° 89-1711, *Bull. civ.* I, n° 127.

- Cass. crim., 16 mai 1991, pourvoi n° 90-82285 ; *Bull. crim.* 1991, n° 208 ; *JCP* 1992, éd. G., I. 3572, obs. G. Viney.

- Civ 1re, 16 juill. 1991, pourvoi n° 90-10.843, *Bull. civ.* I, n° 249 ; *JCP* 1991, éd. G., IV. 367 ; *JCP* 1992, éd. G., I. 3572, obs. G. Viney.

1992
- *Real v. Keen*, 838 *P.2d*. 1073, 314 *Or*. 370 (Or. 1992) (*Real v. Keen*, 112 *Or.App*. 197, 828, *P.2d* 1038 (1992)).
- Cass. crim., 30 janv. 1992, *Graeff, Bull. crim*. 1992, n° 44 ; *JCP* 1992, éd. E., pan. 829 ; *Dr. pénal* août-sept. 1992, comm. 208, pp. 13-14, obs. J.-H. Robert ; *RTD com*. 1992, p. 880, obs. P. Bouzat ; *RTD com*. 1993, p. 151, obs. B. Bouloc.
- CA Douai, 4e ch., 7 oct. 1992, *Juris-Data* n° 1992-49432, *JCP* 1994, éd. E., I. 359, spéc. n° 15, obs. M. Vivant et C. Le Stanc.
- CA Paris, 9e ch. A, 18 nov. 1992, *Juris-Data* n° 023257 ; *JCP* 1994, éd. G., I. 359, spéc. n° 15, obs. M. Vivant et C. Le Stanc.

1993
- CA Paris, 2 février 1993, *Melle Baillie et autres*, *D.* 1993, I.R., p. 118.
- CA Toulouse, 7 déc. 1993, Juris-Data n° 049860.

1994
- Cass. crim. 5 janv. 1994, *JCP* 1994, éd. G., I. 359, spéc. n° 16, obs. M. Vivant et C. Le Stanc**.**

- CA Paris, 9e ch., 15 mars 1994, *Juris-Data* n° 20887 ; *JCP* 1995, éd. E, I. 461, spéc. n° 21, obs. M. Vivant et C. Le Stanc.
- CA Paris, 11e ch. corr., sect. A, 5 avr. 1994, *Assistance Génie Logiciel et Geste c/ Niel et a., Juris-Data* n° 021093 ; *LPA* 5 juill. 1995, n° 80, p. 13 et s., note V. Alvarez ; *JCP* 1995, éd. E., I. 461, n° 20, obs. M. Vivant et C. Le Stanc ; *D.* 1994, IR, p. 130.
- Cass. civ. 3e, 26 mai 1994, pourvoi n° 92-15911, *Bull. civ.* III, n° 110.
- TA Rennes, 6 juill. 1994, *LPA* 24 févr. 1995, p. 12 et s., note F. Mallol.
- CA Paris, 13e ch., 5 oct. 1994 ; *Juris-Data* n° 023667 ; *JCP* 1995, éd. E, I. 461, spéc. n° 21, obs. M. Vivant et C. Le Stanc.
- Cass. crim., 14 déc. 1994, pourvoi n° 92-85.557 ; *Juris-Data* n° 1994-002701 ; *Bull. crim.* 1994, n° 415 ; *JCP* 1995, éd. G., IV. 764 ; *Dr. pénal* avr. 1995, comm. 98, pp. 12-13, obs. J.-H. Robert ; *Rev. sc. crim.* 1995, p. 570, obs. B. Bouloc *; Rev. sc. crim.* 1995, p. 597, obs. J.-C. Fourgoux.
- TGI Paris 17e ch. corr., 16 déc. 1994, *Juris-Data* n° 1994-600554 ; *Expertises* 1995, n° 181, p. 120, note J. Sanqueur.

1995

- *Destination Ventures, Ltd. v. Federal Communications Commission*, 46 *F.3d* 54, spéc. 55 (9th Cir. Feb. 1, 1995).
- CJCE, 7 mars 1995, aff. C-68/93, *Fiona Shevill et al. c/ Press Alliance SA*, *Rec. CJCE* 1995, I, p. 415, *Rev. Crit. DIP* juill.-sept. 1996, p. 487 note P. Lagarde ; *RTD eur.* 1995, p. 611 et s., note M. Gardeñes Santiago, *D.* 1996, jurispr., p. 63 et s., note G. Parléani ; *JDI* 1996, p. 543 et s., obs. A. Huet.
- T. corr. Brest, 14 mars 1995, *LPA* 28 juin 1995, n° 77, note M.- G. Choisy .
- CA Paris, 9e ch. A, 29 mai 1995, *JurisData* n° 1995-022909 ; *Dr. pénal* nov. 1995, comm. 251, p. 7 et s., obs. M. Véron *; Rev. sc. crim.* avr.-juin 1996, p. 379, obs. R. Ottenhof.
- CA Paris, 1er juin 1995, *JurisData* n° 1995-022908, *Rev. sc. crim.* avr.-juin 1996, p. 379, obs. R. Ottenhof.
- CE, 7 juin 1995, *RJDA* 1995, n° 1452, *LPA* 13 avr. 1998, n° 44, p. 9, obs. J.P.M.
- Cass. com. 13 juin 1995, *Petrossian, Dr. sociétés* 1996, comm. 51, obs. Th. Bonneau.
- TGI Paris, 12e ch., 26 juin 1995, *France Telecom c/ Dicko, LPA* 1er mars 1996, n° 27, p. 4 et s., note V. Alvarez.
- CJCE, 19 sept. 1995, aff. C-364/93, *Antonio Marinari c/ Lloyd's Bank et Zubaidi Trading Compagny, Rec. CJCE* 1995. I. p. 2719 et s. ; *Rev. Crit. DIP xxx* 1990, p. 368 et s., note H. Gaudemet-Tallon ; *JDI* 1996, p. 562 et s., note J.-M. Bischoff.
- Cass. crim., 25 oct. 1995, pourvoi n° 94-85.781 ; *Bull. crim.* 1995, n° 320.

1996

- Cass. civ. 1e, 2 avr. 1996, pourvoi n° 94-13.871; *Bull. civ.* I, n° 166 ; 3 juill. 1996, pourvoi n° 94-14.820, *Bull. civ.* I, n° 296 ; *D.* 1996, I.R., p. 194.
- *BMW North America Inc. c/Gore*, 517 *U.S.* 559 (May 20, 1996).
- *Thrifty-Tel, Inc. v. Bezenek*, 46 *Cal. App. 4th* 1559, 54 *Cal.Rptr. 2d*. 468 (Cal.Ct. App., June 28, 1996).
- Cass. crim., 30 oct. 1996, pourvoi n° 94-86042, *Juris-Data* n° 1996-005202.
- *Cyber Promotions, Inc. v. America Online, Inc*., 948 *F. Supp*. 456 (E.D. Pa., Nov. 4, 1996).
- Cass. crim., 28 nov. 1996, *Bull. crim.* 1996, n° 437 ; *JCP* 1997, éd. G., IV. 1214.
- Cass. crim. 4 déc. 1996, pourvoi n° 96-81.163 ; *Juris-Data* n° 1996-005343 ; *Bull. crim.* 1996, n° 445 ; *JCP* 1995, éd. G., IV. 720.
- Cass. crim. 12 déc. 1996, pourvoi n° 95-82198 ; *Juris-Data* n° 005348 ; *Bull. crim.* 1996, n° 465 ; *JCP* 1997, éd. G., IV. 779 ; *RTD com.* 1997, p. 144, obs. B. Bouloc.
- Cass. Crim. 18 déc. 1996, *Rev. sc. crim.* 1998, p. 120, comm. A. Giudicelli.

1997

- Cass. Civ 1re, 14 janv. 1997, *Sté Gordon & Breach Science Publishers, Rev. crit. DIP* 1997, p. 504, note J.-M. Bischoff ; *D.* 1997, p. 177 et s., note M. Santa-Croce ; *JCP* 1997, éd. G., II. 22903, note H. Muir Watt.
- Cass. crim., 30 janv. 1997, pourvoi n° 96-81270, *Juris-Data* n° 1997-001347).
- *CompuServe, Inc. v. Cyber Promotions, Inc.*, 962 *F. Supp*. 1015 (S.D. Ohio, Febr. 3, 1997).
- Cass. civ. 2e, 2 avr. 1997, pourvoi n° 95-14687; *Bull. civ.* II, n° 113.
- *Reno v. ACLU*, 521 *U.S*. 844 (June 26,1997).
- Cass. civ. 1re, 1er juill. 1997, pourvoi n° 95-16.771, *Bull. civ.* I, n° 225.
- Cass. civ. 1e, 8 juill. 1997, *Bull. civ.* I, nos 238 et 239 ; 18 juill. 2000, *Bull. civ.* I, n° 224 ; *D.* 2000, p. 853, note Y. Chartier ; 18 janv. 2005, *Bull. civ.* I, n° 29.
- Cass. civ. 1re 16 juill. 1997, *Époux Wegmann c/ Sté Elsevier Science Ltd*, *JCP* 1997, éd. E., pan. 1087 ; *JDI* 1998, p. 136 et s., obs. A. Huet.
- TGI Privas, 3 sept. 1997, *Rev. sc. crim*. 1998, p. 574, obs. Francillon ; *LPA* 11 nov. 1998, n° 135, p. 19 et s., obs. J. Frayssinet.

1998

- CA Aix-en-Provence, 14 janv. 1998, *Juris-Data* n° 1998-041496.
- CA Caen, 6 mars 1998, *Juris-Data* n° 040489.
- *Hotmail Corp. v. Van$ Money Pie Inc. et al.*, 47 *U.S.P.Q.2d.* 2010, 1998 WL 388389 (N.D.Cal., Apr. 16, 1998).
- Cass, civ. 1re, 16 juill. 1998, pourvoi n° 96-15380, *Bull. civ.* I, n° 260.
- Cass. crim., 21 oct. 1998, pourvoi n° 97-84.414, *inédit.*
- *Am. Online, Inc. v. IMS et al., 24 F.Supp. 2d* 548 (E.D.Va., oct. 29 1998).
- *Am. Online, Inc. v. LCGM, Inc. et al*., Civ. Act. N° 98-102-A, 46 *F. Supp.2d*. 444 (E.D. Va., Nov. 10, 1998).

1999

- Cass. Ass. plén., 26 mars 1999, pourvoi n° 95-20640 ; *Juris-Data* n° 001247 ; *Bull. Ass. plén.*, n° 3, p. 3 ; *JCP* 2000, éd. G., I. 199, spéc. n° 12, note G. Viney.
- Cass. civ.1re., 13 avr. 1999, *Juris-Data* n° 1999-001623, *Contrats. conc. conso*. sept. 1999, comm. 127, p. 1819, obs. L. Leveneur.
- Cass. civ. 1re, 11 mai 1999, *Mobil North Sea*, *JCP* 1999, éd. G., II. 10183, note H. Muir Watt ; *D.* 1999, somm., pp. 295-296, obs. B. Audit ; *Rev. crit. DIP* avr.-juin 2000, p. 199 et s., note J.-M. Bischoff ; *JDI* 1999, p. 1048 et s., note G. Légier
- Cass. com., 18 mai 1999, pourvoi n° 96-19235, *inédit*
- Cass. crim., 30 juin 1999, *Bull. crim.* 1999, n° 170 ; *D.* 1999, IR, p. 224.
- CA Paris, 16 sept. 1999, *Juris-Data* n° 1999-094960.
- Cass. crim., 26 oct. 1999, pourvoi n° 98-84.446 ; *Juris-Data* n° 1999-004316 ; *Bull. crim.*, n° 233 ; *Rev. sc. crim.* 2000, p. 384, obs. B. Bouloc ; *D.* 2000, AJ, p. 80.
- Crim. 27 oct. 1999, pourvoi n° 98-86.017 ; *Juris-Data* n° 199-004318, *Bull. crim.*, n° 235.
- Cass. crim. 8 déc. 1999, pourvoi n° 98-84752, *Bull. crim.* 1999, n° 296.
- CA Paris, 9e ch. A, 15 déc. 1999, *D.* 2000, IR, P. 44 ; *Comm. com. électr*. juill.-août 2000, pp. 30-31 ; *Gaz. Pal.* 23 janv. 2001, n° 23, p. 39 et s., note V. Prat.

2000

- Cass. crim. 14 mars 2000, pourvoi n° 99-85.147.
- *eBay, Inc., v. Bidder'sEdge, Inc.*, 100 *F. Supp. 2d.* 1058 (N.D. Cal., May 24, 2000).
- *Ticketmaster Corp. v. Tickets.com, Inc.* n° 99CV7654, 2000 WL 1887522, *1 (C.D. Cal., Aug. 10, 2000).
- CA Paris, 1re ch. B, 15 sept. 2000, *SNC Hachette Filipacchi c/ Larissa Vadko-Zschech, Gaz. Pal.* 26-27 sept. 2001, 2, somm., p. 1527, note D. Amson.
- CA Rennes, 28 sept. 2000, 3e ch. corr., *Juris-Data* n° 2000-141862, *JCP* 2001, éd. G., II, 10592, note C. T. Geffroy et P. Belloir.

- *Am. Online, Inc. v. National Health Care Discount, Inc.*, 121 *F. Supp. 2d.* 1255 (N.D. Iowa, Sept. 29, 2000).
- Cass. civ. 1re, 3 oct. 2000, *Juris-Data* n° 006126 ; *Resp. civ. et assur.* janv. 2001, comm. 6, p. 13.
- Cass. crim. 17 oct. 2000, pourvoi n° 00-80.148.
- Cass. crim., 28 nov. 2000, pourvoi n° 99-87.262.
- CA Paris, 9e ch. corr., sect. A, 6 déc. 2000, *Juris-Data* n° 134502 ; *Comm. com. électr*. mars 2001, comm. 28, pp. 23-24, obs. C. Le Stanc.
- *Register.com, Inc. v. Verio, Inc.*, 126 *F. Supp. 2d.* 238, spéc. 241, 255 (S.D.N.Y., Dec. 12, 2000).

2001
- TGI Lyon, 1re ch. corr., 20 févr. 2001, *Claranet c/ Patrice C., Comm. com. électr.* janv. 2002, comm. n° 5, p. 28, obs. C. Le Stanc ; *Gaz. Pal.* sept.-oct. 2001, 2, somm., p. 1686, note A. Blanchot.
- TGI Rochefort-sur-Mer, 28 févr. 2001, *Monsieur Christophe G c/ SA France Telecom Interactive*, *Juris-Data* n° 2001-199479 ; *Legalis.net* 2002, n° 3, spéc. p. 114 ; *JCP* 2003, éd. E., chron., 147, spéc. n° 30, obs. J.-M. Bruguière et V. Nisato ; *Comm. com. électr*. avr. 2002, comm. 59, pp. 24-25, obs. L. Grynbaum.
- CA Paris, 1er oct. 2001, *Juris-Data* n° 2001-163093.
- CA Aix-en-Provence, 9 oct. 2001, Juris-Data n° 2001-170316.
- Cass. civ. 2e, 25 oct. 2001, *inédit*, pourvoi n° 99-16942 ; *Juris-Data* n° 2001-011536 ; *Resp. civ. et assur*. janv. 2002, comm. 12, p. 16.
- Cass. crim. 30 oct. 2001, pourvoi n° 99-82136, inédit.
- Cass. crim., 7 nov. 2001, pourvoi n° 01-80592 ; *Bull. crim.* 2001, n° 230 ; *RTD civ*. 2002, p. 314, obs. P. Jourdain ; *LPA* 16 oct. 2002, n° 207, p. 15 et s., note B. Jaluzot.

2002
- TGI Paris, ord. réf., 15 janv. 2002, *Monsieur P. V. c/ Sté Liberty Surf et Sté Free*, Juris-*Data* n° 2002-188900 ; *D.* 2002, jurispr., p. 1544 et s., note L. Marino ; *Comm. com. électr*., avr. 2002, 2e esp., comm. 59, p. 24 et s., note L. Grynbaum ; 2003, éd. E., chron., 147, spéc. n° 30, obs. J.-M. Bruguière et V. Nisato.
- Cass. crim. 20 févr. 2002, *Bull. civ.* 2002, n° 37 ; *D.* 2003, somm., p. 248, obs. S. Mirabail.
- Cass. civ. 1re, 9 avr. 2002, pourvoi n° 00-13.314 ; *Juris-Data* n° 2002-013914 ; *Bull. civ.* I, n° 116.
- TGI Paris, 12e ch., 24 mai 2002, *Lyonnaise Communications c/ M. Philippe P., Comm. com. électr.* juill.-août 2002, actu. 107, p. 4, obs. G. Haas
- *Verizon Online Services, Inc. v. Ralsky*, 203 *F. Supp.2d* 601 (E.D.Va., June 7, 2002).
- TGI Paris, 17e ch., 2e sect., 10 juill. 2002, *Anne D. c/ Société Wanadoo*, disponible sur : http://legalis.net/jurisprudence-decision.php3?id_article=137.
- Cass. civ. 2e, 26 sept. 2002, pourvoi n° 00-18627 ; *Juris-Data* n° 2002-015653 ; *Bull. civ.* II, n° 198 ; *Resp. civ. et assur.* déc. 2002, comm. 351, p. 14 ; *RTD civ.* 2003, p. 100 et s., obs. P. Jourdain.
- CA Paris, 11 octobre 2002, n° RG : 2002/09099 (confirmant TGI Paris, ord. réf., 15 janv. 2002, *Monsieur P. V. c/ Sté Liberty Surf et Sté Free*, arrêt préc.).
- CA Paris, 12e ch., sect. A, 30 oct. 2002, *Antoine C. c/ Min. pub., Sté Tati*, *Juris-Data* n° 2002-212825 ; *Comm. com. électr.* janv. 2003, comm. 5, pp. 31-32, note L. Grynbaum ; *Expertises* 2003, n° 266, p. 27 et s., note C. Morel.
- CA Paris, 12e ch. B, 18 déc. 2002, *D.* 2002, I.R., p. 940.

2003
- Cass. civ. 2e, 23 janv. 2003, pourvoi n° 01-00.200, *Bull. civ.* II, n° 20 ; *JCP* 2003, éd. G., II. 10110, note J.-F. Barbieri ; *D.* 2005, I.R., p. 605.
- CA Paris, 25e ch. A., 28 févr. 2003, *Gaz. Pal.* 16 et 17 mai 2003, n° 137, p. 25.
- CA Toulouse, 15 avr. 2003, *M. Barthez c/ Sté Hachette Filipacchi Associés, inédit*.

- Cass. com. 6 mai 2003, *Ducasse*, pourvoi n° 00-18.192, *Juris-Data* n° 2003-018973, *D.* 2003, jurispr., p. 2228, note G. Loiseau ; *Comm. com. électr*. juill.-août 2003, comm. 70, note C. Caron*; JCP* 2003, éd. G., II. 10169, note E. Tricoire ; *RTD civ*. 2003, p. 679, obs. J. Hauser.
- TGI Paris, réf., 26 mai 2003, *SNES* c/ *La Droite Libre et al.*, RG n° 03/54806 , *Comm. com. électr*. juillet-août 2003, comm. n° 78, note A. Lepage, p. 40 et s.
- Cass. civ. 1re, 27 mai 2003, pourvoi n° 89-17.602 ; *Bull. civ.* I, n° 129.
- T. com Grenoble, ord., 4 juin 2003, *Bouchard Th. c/ All Systems Maisonnet Aisonnet Allomaison*, rôle n° 031P00887
- TGI Paris, 6 juin 2003, *Ministère public et M. Thomas QUINOT c/ M. R.G.U.*
- Cass. civ. 3e, 12 juin 2003, *D.* 2004, p. 523, note S. Beaugendre.
- Cass. civ. 2e, 19 juin 2003 (2 arrêts), pourvois n° 01-13289 et 00-22302 ; *Bull. civ*. I n° 203 ; *D.* 2003, jurispr., p. 2326, note J.-P. Chazal ; *RTD* civ. 2003, p. 716, n° 3, note P. Jourdain.
- *Intel Corp. v. Hamidi*, 30 *Cal. 4th* 1342, 71 *P.3d* 2961, 1 *Cal.Rptr. 3d*. 32 (June 30, 2003).
- Cass. crim., 23 sept. 2003, *inédit, Juris-Data* n° 2003-020922, pourvoi n° 02-84623.
- Cass. crim., 8 oct. 2003, pourvoi n° 02-80.449.

- Cass. civ. 1re, 28 oct. 2003, *Pays Fourvel c/ Sté Axa courtage et al., Rev. crit. DIP* janv.-mars 2004, p. 83 et s., note D. Bureau ; *JDI* 2004, p. 499 et s., note G. Légier ; *JCP* 2004, G., II. 10006, note G. Lardeux
- TGI Mans, ch. corr., 7 nov. 2003, *Sté Smith et Nephew c/ M. L., Gaz. Pal.* 20 juill. 2004, n° 202, p. 44, note É. Barbry.
- Cass. civ. 2e, 20 nov. 2003, *Juris-Data* n° 2003-020895 ; pourvoi n° 01-17977 ; *Bull. civ.* II, n° 355 ; *D.* 2003, p. 2902 et s., concl. R. Kessous et note L. Grynbaum et 2004, somm., p. 1346, obs. D. Mazeaud ; *JCP* 2004, éd. G., I. 163, spéc. n° 36, obs. G. Viney ; *RTD civ.* 2004, p. 103 et s., obs. P. Jourdain.
- Cass. civ. 3e, 3 déc. 2003, pourvoi n° 02-18.033 ; *Juris-Data* n° 2003-021222 ; *Bull. civ.* III, n° 221; *JCP* 2004. I. 163, chron. G. Viney ; *RTD civ*. 1994, p. 295 et s., note P. Jourdain.
- *Missouri ex rel. Nixon v. American Blast Fax, Inc.,* 196 *F. Supp.2d* 920 (E.D. Mo. 2002), *rev'd*, 323 *F.3d* 649 **(**8th Cir. 2003).

2004

- Cass. civ. 1re, 9 mars 2004, pourvoi n° 01-17. 277 ; *Bull. civ.* I, n° 79.
- CA Pau, 1re ch. corr., 14 avr. 2004, *Juris-Data* n° 2004-240039 ; *JCP* 2004, éd. G., IV. 2995.
- T. com. Paris, 6e ch., 5 mai 2004, *Microsoft Corp. et AOL France c/ monsieur K., Gaz. Pal*. 12 oct. 2004, n° 286, p. 36, note E. Garnier ; *Comm. com. électr*. déc. 2004, comm. 164, note P. Stoffel-Munck.
- Cass. civ. 3e, 3 juin 2004, pourvoi n° 03-11.475 ; *Juris-Data* n° 2004-023963 ; *Resp. civ. et assur*. sept. 2004, comm. 256, p. 22.
- CJCE, 10 juin 2004, aff. C-168/02, *Rudolf Kronhofer, D.* 2005. pan., p.1268, obs. P. Courbe et H. Chanteloup ; *Rev. crit. DIP* avr.-juin 2005, p. 326, note H. Muir Watt.
- CA Paris, 9e ch. corr., sect. B, 17 sept. 2004, *Juris-Data* n° 2004-255097.
- Cass. crim. 28 sept. 2004, pourvoi n° 03-86604, *Bull. crim*, n° 224, p. 801.
- Cass. civ. 2e, 7 oct. 2004, pourvoi n° 02-14399.
- Cass. crim., 19 oct. 2004, pourvoi n° 04-82218, *Juris-Data* n° 2004-025542 ; *Bull. crim*. 2004, n° 245.
- Cass. civ. 1re, 9 nov. 2004, pourvoi n° 02-12.506, *Bull. civ.* I, n° 264, p. 220.
- CA Aix-en-Provence, 2e ch., 25 nov. 2004, *D.* 2005, p. 845 et s., note Didier Poracchia et Claude-Albéric Maetz.
- TGI Paris, 17e ch., 7 déc. 2004, *Ministère Public c/ Fabrice H., RLDI* mai 2005, n° 141, p. 28 et s., note J. Le Clainche.

2005

- CA Paris, 4 févr. 2005, 14e ch., *BNP Paribas c/World Press Online*, RG n° 04/55398, disponible sur :
http://www.foruminternet.org/telechargement/documents/ca-par20050204.pdf.

- CA Paris, 11e ch. sect. B, 18 mai 2005, *Fabrice H. c/ Ministère public, inédit*.
- Cass. civ. 2e, 2 juin 2005, pourvoi n° 03-20.011, *Juris-Data* n° 2005-028683 ; *Bull. civ.* II, n° 146 ; *JCP* 2005, éd. G., IV. 2622.
- CA Toulouse, 3e ch. corr., 12 juin 2005, *Juris-Data* n° 2005-272643.
- CA Douai, 14 juin 2005, *Juris-Data* n° 2005-278037
- Cass. civ. 3e, 28 juin 2006, pourvoi n° 04-20040 ; *Bull. civ.* III, n° 164 ; *RTD civ.* 2006, p. 770, obs. P. Jourdain.
- Cass. ass. plén., 8 juill. 2005, pourvoi n° 97-83.023 ; *JurisData* n° 2005-029430 ; *Bull. crim.*, n° 2, p. 10 *; JCP* 2005, éd. G., IV. 2999.
- Cass. civ. 2e, 13 juill. 2006, pourvoi n° 05-16645, *RTD civ.* 2007, p. 128, obs. P. Jourdain.
- Cass. crim., 7 sept. 2005, *inédit*, pourvoi n° 04-87548; *Juris-Data* n° 2005-030008.
- CA Versailles, 12e ch., 2e sect., 22 sept. 2005, *SAS Calendriers Jean Lavigne c/ Sté Universal Music*, *Juris-Data* n° 2005-288693; *Comm. com. électr.* janv. 2006, comm. 4, p. 29 et s., note C. Caron ; *Legipresse* 2006, III, p. 109, comm. J.-M. Bruguière ; *D.* 2006, p. 2705, obs. L. Marino.

2006

- Cass. crim., 14 mars 2006, *Fabrice X. c/ Ministère Public*, pourvoi n° 05-83.423, *Bull. crim.* 2006, no 69 ; *Comm. com. électr.* sept. 2006, comm. 131, p. 43 et s., note A. Lepage ; *D.* 2006, p. 1066 ; *JCP* 2006, éd. G., IV. 1819, *RLDI* mai 2006, n° 471, p. 34 et s., note J. Le Clainche et *RLDI* juin 2006, no 498, p. 28 et s., note Ph. Belloir.
- T. com. Nanterre, 15 mars 2006, *LBVH c/ Wanadoo*, RG : 2004F01632.
- TGI Paris, 12e ch., 19 mai 2006, *Ministère Public c/ Clément P. et al.*, *Gaz. Pal.* 18 janv. 2007, n° 18, p. 35, note J.-F. Forgeron et A. Fiévée, disponible sur : http://www.legalis.net/spip.php?page=jurisprudence-decision&id_article=1714.
- Cass. crim. 29 mars 2006, *Juris-Data* n° 2006-033128, *Comm. com. électr.* juill.-août 2006, comm. 117, pp. 39-40, note É. A. Caprioli.
- TGI Nanterre, 8 juin 2006, *Soc Amen c/ Michel M.*, *RLDI* mars 2007, n° 828, p. 46, disponible sur : http://www.legalis.net/jurisprudence-decision.php3?id_article=1868.
- Cass. crim. 20 juin 2006, pourvoi n° 05-86.491, *inédit*.
- *United States of America (for the FTC), Plaintiff, v. Xanga.com, Inc., a corporation, John Hiler, individually and as an officer of the corporation, and Marc Ginsburg, individually and as an officer of the corporation, Defendants (U.S. District Court for the Southern District of New York)*, Civil Action n° 06-CIV-6853(SHS), FTC n° 062-3073, 7 sept. 2006.
- Cass. crim., 12 sept. 2006, pourvoi n° 05-87.609, *Juris-Data* n° 2006-035232 ; *Dr. pénal* déc. 2006, p. 22, note M. Véron.
- Cass. crim., 13 sept. 2006, pourvoi n° 05-81.737; *Juris-Data* n° 2006-035236 ; *Bull. crim.*, n° 221, p. 784 ; *Dr. pénal* déc. 2006, comm. 158, note M. Véron ; *JCP* 2007, éd. G., II. 10033, note J. Lasserre-Capdeville ; *RTD com.* 2007, p. 248, obs. B. Bouloc ; *RTD civ.* 2007, p. 350, obs. J. Mestre et B. Fages.
- TGI Paris, 3e ch., 2e sect., 28 sept. 2006, *E. Thomas et 2 Secondes production c/ Réservoir Prod.*, *Legipresse* 2006, I, p. 160 et s. et *ibid.* 2007, II, p. 18 et s., obs. Th. Hass ; *Ibid.* mars 2007, III, p. 54 et s., note J.-M. Bruguière.
- Cass. civ. 1re, 24 oct. 2006, pourvoi n° 04-17.560, *Sté VF Films Production et Sté Nationale de télévision France 3 c/ X*, *Juris-Data* n° 2006-035517 ; *Legipresse* déc. 2006, I, p. 172 et *Legipresse* janv.-févr. 2077, III, p. 1, note L. Marino.
- Cass. civ. 1re, 21 nov. 2006, pourvoi n° 05-15674 ; *Bull. civ.* I, n° 498 ; *JCP* 2006, éd. G., IV. 3475 ; *JCP* 2007, éd. G., I. 115, spéc. n° 2, obs. P. Stoffel-Munck.
- CA Aix-en-Provence, 6 déc. 2006, *Juris-Data* n° 2006-325519.

2007

- Cass. civ 1re, 23 janv. 2007, *Caisse d'épargne De Sarrebruck*, *Rev. crit. DIP* oct.-déc. 2007, p. 760 et s., note O. Boskovic ; *D.* 2007, études, p. 1244 et s., note N. Bouche.

- Cass. civ 1re, 30 janv. 2007, *M. Lamore c/ Universal Studios Inc. et autres*, *Rev. crit. DIP* oct.-déc. 2007, p. 769, note T. Azzi.
- CA Paris, 31 janv. 2007, *JurisData* n° 2007-340182
- TGI Montauban, 9 mars 2007, *SCPP c/ Marie-Thérèse O., inédit*, disponible sur le site <legalis.net>.
- Cass. com., 13 mars 2007, *inédit*, pourvoi n° 05-20.606, *LPA* 11 sept. 2007, n° 182, p. 7 et s., note M.-L. Lanthiez.
- Cass. civ. 1re, 27 mars 2007, 1re ch., *Bureau Veritas*, pourvoi n° 05-10.480 ; *Juris-Data* n° 2007-038216 ; *Resp. civ. assur.* juin 2007, comm. 194, p. 22 et s. ; *D.* 2007, actu., p. 1074 et s., obs. I. Gallmeister ; *Rev. crit. DIP* avr.-juin 2007, p. 405 et s. , note D. Bureau ; *JDI* 2007, p. 949, note G. Légier.
- Cass. crim., 27 mars 2007, pourvoi n° 06-85.442 ; *Juris-Data* n° 2007-038470 ; *Bull. crim.*, n° 94 ; *Dr. pénal* juin 2007, comm. 87, obs. J.-H. Robert ; *D.* 2007, p. 1336, obs. C. Rondey.
- CA Paris, 13e ch., sect. B, 27 avril 2007, *Juris-Data* n° 2007-338935.
- CA Paris, 13e ch., sect. A, 15 mai 2007, *S. c/ Ministère Public et autres*, RG n° 06/01954, *Juris-Data* n° 2007-336454, *Comm. com. électr.* déc. 2007, comm. 144, p. 32 et s., note C. Caron.
- CE, 23 mai 2007, n° 288149, *Sté des auteurs compositeurs et éditeurs de musique et a.*, *Juris-Data* n° 2007-071900 ; *Comm. com. électr.* juill. 2007, comm. 90, p. 28 et s., note C. Caron ; *JCP* 2007, éd. G, I. 176 ; *Propr. intell.* juill. 2007, n° 24, pp. 334-335, obs. J.-M. Bruguière ; *Expertises* 2007, n° 316, pp. 263-264, note L. Walker ; *Légipresse* juill.-août 2007, III, n° 243, III, p. 141 et s., note J. Frayssinet.
- TGI Paris, 1er juill. 2007, *Comm. com. électr.* mars 2008, comm. 46, p. 42 et s., note É. A. Caprioli.
- TGI Saint-Brieuc, 6 sept. 2007, *Ministère Public, et al. c/ P., inédit*, *RLDI* oct. 2007, n° 1028, p. 26 et s., obs. L. Costes et J.-B. Auroux.
- TGI Roche-sur-Yon, 24 sept. 2007, *Ministère public c/ Frank A. et al.*, *Comm. com. électr.* déc. 2007, comm. 158, pp. 45-46, note É. A. Caprioli.
- Cass. crim. 3 oct. 2007, pourvoi n° 07-81.045 ; *Bull. crim.*, n° 236 ; *D.* 2007, AJ, p. 2807 ; *Rev. sc. crim.* 2008. 99, obs. J. Francillon ; *AJ pénal* 2007, p. 535, obs. G. Royer ; *RTD com.* 2008, p. 433, obs. B. Bouloc ; *Dr. pénal* déc. 2007, comm. 158, pp. 37-38, obs. M. Véron.
- Cass. crim., 16 oct. 2007, pourvoi n° 06-88015, *JurisData* n° 2007-041527.
- T. corr. Strasbourg, 11 déc. 2007, v. le site disponible sur : http://www.01net.com/editorial/367148/prison-ferme-pour-escroquerie-a-la-nigeriane/.
- CA Rennes, 3e ch., 20 nov. 2007, *Ministère public, F., G. /MM. A. B. C. D. E*, disponible sur : http://www.legalis.net/spip.php?page=jurisprudence-decision&id_article=2291.
- TGI Paris, ord. réf., 24 déc. 2007, *Techland c/ France Télécom et autres*, *RLDI* févr. 2008, n° 1167, p. 27 et s., note L. Costes et J.-B. Auroux, disponible sur le site <legalis.net>.

2008

- *Jeremy Jaynes v. Commonwealth of Virginia*, 666 *S.E.2d* 303, 276 *Va.* 443 spéc. 450 (2008).
- CJCE, 29 janv. 2008, *Productores de Música de España (Promusicae) c/ Telefónica de España SAU*, Aff. C-275/06, *JCP*, éd. G, 2008, II. 10099, note E. Derieux ; *Comm. com. électr.* mars 2008, comm. 32, p. 25 et s., note C. Caron ; *D.* 2008. AJ. 480, obs. J. Daleau ; *RTD com.* 2008, p. 302, obs. F. Pollaud-Dulian.
- CJCE, 19 févr. 2009, *LSG c/ Tele 2 Telecommunication*, aff. C-557/07, *Dalloz Actualités* 13 mars 2009, comm. J. Daleau.
- CE, ord. réf., sect. contentieux, 19 févr. 2008, réq. n° 31194, *Profil France*, *Juris-Data* n° 2008-073370.
- TGI Rennes, 21 févr. 2008, *Comm. com. électr.* juin 2008, comm. 8, pp. 45-46, note É. A. Caprioli.
- Cass. crim., 19 mars 2008, *inédit*, pourvoi n° 07-86.137 ; *Juris-Data* n° 2008-043756.
- CA Pau, ch. corr., 3 avr. 2008, *Juris-Data* n° 2008-369964 ; *JCP* 2008, éd. G., IV. 2871.
- Cass. Com., 8 avr. 2008, pourvoi n° 07-10939, *inédit*.

- CA Paris, 13e ch., 5 mai 2008, *Juris-Data* n° 2008-362810.
- CA Paris, 13e ch. 16 mai 2008, *Juris-Data* n° 2008-364022.
- CA Rennes, 3e ch. crim., 22 mai 2008, *SACEM, SDRM et Ministère Public c/ Cyrille S.*, RG no 07/01495.
- TGI Lyon, ch. corr., 27 mai 2008, *Comm. com. électr.* mars 2009, comm. 30, p. 45 et s., note É. A. Caprioli.
- CA Paris, 3e ch. instr., 28 mai 2008, RG n° 2007-01064, *Dr. pénal* déc. 2008, Étude 27, p. 24 et s., note L. Flament.
- CA Rennes, 3e ch., 23 juin 2008, *L. T. c/ Ministère public*, no 07/01021, *RLDI* juill. 2008, no 40, p. 17 et s., note L. Costes.
- Cass. com. 24 juin 2008, *Beau*, pourvois nos 07-10.756 et 07-12.115, *Bull. Joly* 2008, p. 953, note G. Loiseau ; *D.* 2008. 2569, note A. Mendoza-Caminade; *JCP* 2008, éd. E., 2466, note C.-A. Maetz; *Rev. Sociétés* 2009, p. 587, note G. Parléani ; *Droit* des *sociétés* 2009, comm. 23, note M.-L. Coquelet ; *Comm. com. électr.* déc. 2008, comm. 133, p. 31 et s., note C. Caron.
- CA Chambéry, 2 juill. 2008, *Juris-Data* n° 2008-370873.
- CA Reims, ch. appels corr., 20 août 2008, RG n : 08/00579, *Juris-Data* : 2008-008914.
- Cass. civ. 2e, 11 sept. 2008, *RDC* 2009, p. 77, obs. O. Deshayes.
- CA Pau, 18 sept. 2008, *Juris-Data* n° 2008-372637 –
- TGI Paris, 31e ch., 18 sept. 2008, *Éditions Neressis c/ Arkadia, Stéphane V. C., Comm. com. électr.* janvier 2009, n° 1, comm. 10, p. 48 et s., note É. A. Caprioli.
- CA Douai, 13e ch., 29 sept 2008, *Juris-Data* n° 2008-371368
- CA Lyon, ch. corr., 29 oct. 2008, *Juris-Data* n° 2008-371645
- CA Paris, 21 nov. 2008, *Juris-Data* n° 2008-005949.
- CA Paris, 26 nov. 2008, *Juris-Data* n° 2008-374091.
- Cass. civ. 1re, 11 déc. 2008, n° 07-19.494, F P+B, *Brossard-Martinez c/ Sté Photoalto*, *JCP* 2009, éd. G., II. 10025, G. Loiseau.
- *United States of America (For the FTC), Plaintiff, v. Sony Bmg Music Entertainment, a general partnership subsidiary of Sony Corporation of America, Defendant (U.S. District Court For the Southern District of New York)*, Case n° 08 CV 10730 (LAK), FTC File n° 082 3071, 11 déc. 2008, disponible sur : http://www.ftc.gov/os/caselist/0823071/index.shtm et http://www.ftc.gov/opa/2008/12/sonymusic.shtm.

2009

- Cass. crim. 13 janv. 2009, *SACEM et autres c/ Cyrille Y.*, pourvoi no 08-84.088, *D.* 2009, AJ, p. 497, obs. J. Daleau ; *Droit pénal* mai 2009, Étude 10, p. 5, note L. Flament ; *RTD com.* 2010, p. 310, note F. Pollaud-Dulian ; *Comm. com. électr.* avril 2009, comm. 31, p. 25 et s., note C. Caron.
- Civ. 2e, 22 janv. 2009, pourvois n° 07-20878 08-10392 ; *Bull. civ.* II, n° 26 ; *D.* 2009, p. 1114, note R. Loir.
- CA Douai, 29 janv. 2009, *Juris-Data* n° 2009-376104.
- CA Grenoble, 23 févr. 2009, *Juris-Data* n° 2009-377045.
- Cass. crim., 11 mars 2009, pourvoi n° 08-83.401 ; *Juris-Data* n° 2009-047746 ; *Dr. pénal* juin 2009, comm. 81, p. 31, note M. Véron.
- Cass. Crim. 24 mars 2009, pourvoi n° 08-86.530, *Juris-Data* n° 2009-047943 ; *Dr. Pénal* juin 2009, comm. 84, p. 34 et s., obs. J.-H. Robert ; *Cont. conc. Conso.* août-sept. 2009, comm. 235, pp. 39-40, obs. G. Raymond.
- Cass. civ. 1re, 25 mars 2009, pourvoi n° 07-20774 ; *Bull. civ.* I, n° 70.
- Cass. civ. 2e, 9 avr. 2009, arrêt préc., *JCP* 2009, éd. G., IV. 1831 ; *LPA* 23 juill. 2009, n° 146, p. 18 et s., note A. Dumery.
- Cass. crim., 15 juin 2009, pourvoi n° 08-88560, *RLDI* sept. 2009, n° 1507, p. 16 et s., note L. Costes et M. Trézéguet.
- CA Aix-en-Provence, 7e ch., sect. A, 30 juin 2009, Juris-Data n° 2009-014406, *Comm. com. électr.* mars 2010, comm. 27, p. 33 et s., note A. Lepage

- TGI Paris, ord. réf. 25 juin 2009, *Vernes c/* SAS *Les Échos, Légipresse* nov. 2009, n° 266, p. 215 et s., note N. Mallet-Poujol.
- Cass. civ. 3e, 8 juill. 2009, pourvoi n° 08-10869, *Bull . civ.* III, n° 170.
- CA Paris, 9 sept. 2009, *Damien B. c/ Forever Living Products France, Comm. com. électr.* déc. 2009, comm. 120, pp. 47-49, note É. A. Caprioli.
- Cass. crim. 30 sept. 2009, pourvoi n° 09-80.373 ; *Juris-Data* n° 2009-049991 ; *Bull. crim.* n° 162, *Comm. com. électr.* déc. 2009, comm. 115, note A. Lepage.
- Cass. crim, 6 oct. 2009, pourvoi n° 08-87.757, *Juris-Data* n° 2009-05010171 ; *Dr. Pénal* juin 2009, comm. 153, p. 37 et s., obs. J.-H. Robert.
- Cass. civ. 2e, 8 oct. 2009, pourvoi n° 08-18492, *inédit.*
- CE, sect. contentieux, 6 nov. 2009, n° 304300, *Sté Inter Confort, Juris-Data* n° 2009-012926, *Comm. com. électr.* févr. 2010, p. 42 et s., note É. A. Caprioli.
- Cass. crim. 15 déc. 2009, pourvoi n° 09-83.059 ; *Juris-Data* n° 2009-050976 ; *Bull. crim.*, n° 212 ; *D.* 2010, p. 203, note X. Depech ; *Dr. pénal* mars 2010, comm. 41, pp. 59-60, note J.-H. Robert ; *AJ Pénal* 2010, p. 73, note N. Éréséo et J. Lasserre Capdeville ; *Rev. sc. crim.* janv.-mars 2010, p. 146 et s., note C. Ambroise-Castérot.

2010
- CA Paris, 1er févr. 2010, 12e ch., *Cyrille S. c/ SACEM, SDRM*, disponible sur le site <legalis.net>.
- CJCE, 11 mars 2010, aff. C-19/09, *Wood Floor Solutions Andreas Domberger GmbH v. Silva Trade SA*, *JCP* (17/06) 2010, éd. E., alerte 1579, note M. Fernet.
- Cass. crim., 8 avr. 2010, pourvoi n° 09-83961, *inédit*.
- Cass. civ. 1re, 1er déc. 2010, pourvoi n° W09-13.303.

NOTES ET OBSERVATIONS DE JURISPRUDENCE

AMBROISE-CASTEROT (C.)
note sous Cass. crim. 15 déc. 2009, *Rev. sc. crim.* janv.- mars 2010, p. 146 et s.

AUDIT (B.)
note sous sous CJCE, 5e ch., 27 sept. 1988, aff. préc., *JDI* 1989, p. 457 et s.

BLANCHOT (A.)
note sous TGI Lyon, 1re ch. corr., 20 févr. 2001, *Gaz. Pal.* sept.-oct. 2001, 2, somm., p. 1686.

BOSKOVIC (O.)
note Cass. civ 1re, 23 janv. 2007, *Caisse d'épargne De Sarrebruck, Rev. crit. DIP* oct.-déc. 2007, p. 760 et s.

BRUGUIERE (J.-M.)
note sous TGI Paris, 28 sept. 2006, *Evelyne THOMAS et 2 Secondes Production*, jugement préc., *Légipresse* mars 2007, n° 239, p. 54 et s.

BRUGUIERE (J.-M.) et GLEIZE (B.)
obs. sous Cass. civ. 1re, 25 janv. 2000, pourvoi n° 97-15.163, *X c/ Sté Presse Alliance et a.* ; *Juris-Data* n° 2000-000257.

CARON (C.)
- note sous CA Versailles, 22 sept. 2005, *SAS Calendriers Jean Lavigne c/ Sté Universal Music et al., Com. comm. électr.* janv. 2006, comm. 4, p. 29 et s.
- note sous Cass. crim., 13 janv. 2009, *SACEM et autres c/ Cyrille Y., Comm. comm. électr.* avril 2009, comm. 31 p. 25 et s.

COSTES (L.) ET AUROUX (J.-B.)
obs. sous TGI Saint-Brieuc, 6 sept. 2007, *Ministère Public, et al. c/ P., inédit, RLDI* oct. 2007, n° 1028, p. 26 et s.

FOURGOUX (J.-C .)
note sous Cass. crim., 8 déc. 1987, *Rev. sc. crim.* oct.-déc. 1988, p. 808.

GAUDEMET-TALLON (H.)
note sous CJCE, 5e ch., 27 sept. 1988, *Rev. crit. DIP* janv.-mars 1989, p. 112 et s.

JOURDAIN (P.)
note sous Cass. civ. 2e, 8 févr. 1989, *RTD civ.* 1989, p. 556 et s.

JOURDAIN (P.)
obs. sous Cass. civ. 1re, 7 juin 1989, *RTD* civ. 1992, spéc. pp. 113-114.

LEPAGE (A.)
- note sous Cass. crim. 14 mars, 2006, *Fabrice X. c/ Ministère Public, Comm. com. électr.* sept. 2006, comm. 131, p. 43 et s.
- note sous CA Paris, 14e ch. A, 13 sept. 2000, *D.* 2001, somm., p. 2079.

LINDON (R.)
note sous CA Paris, 13 févr. 1971, *JCP* 1971, éd. G., II. 16774.

LOISEAU (G.)
- note sous Cass. civ. 1re, 13 janv. 1998, *D. c/ Sté Jag., JCP* 1998, éd. *G.*, II. 10082.
- note sous Cass. civ. 1re, 11 déc. 2008, *JCP* 2009, éd. G., II. 10025.

MALAURIE (P.)
note sous Cass. civ. 1re, 30 mai 1967, *Kieger, D.* 1967, jurispr., p. 629 et s.

MARINO (L.)
note sous TGI Paris, ord. réf., 15 janv. 2002, *Monsieur P. V. c/ Sté Liberty Surf et Sté Free, D.* 2002, jurispr., p. 1544 et s.

POLLAUD-DULIAN (F.)
- note sous Cass. com. 27 févr. 1990, *Mazenod, JCP* 1990, éd. G., II. 21545).
- note sous TGI Paris, 17 sept. 2004, RG n° 02/15485, *Inès de la Fressange, JCP* 2004, éd. G., II. 10182.

PUTMAN (E.)
note sous CA Saint-Denis-de-la-Réunion, 6 oct. 1989, *JCP* 1990, éd. G., II. 21504.

RASCHEL (L.)
note sous Cass. civ. 1re, 14 janv. 2010, pourvois n° 08-16.760 et 08-21.562 ; *JCP* 2010, éd. G., note 413, p. 763 et s.

RAVANAS (J.)
note sous Cass. civ. 1e, 20 nov. 1990, *Mme Monanges c/ Kern et a., JCP* 1992, éd. G., II. 21908.

SIALELLI (J.-B.)
obs. sous Cass. civ. 1re, 19 oct. 1959, *JDI* 1960, p. 486.

TRICOIRE (E.)
note sous Cass. com., 6 mai 2003, *JCP* 2003, éd. G., II. 10169.

VINEY (G.)
- note sous Cass. Ass. plén., 26 mars 1999, pourvoi n° 98-84.446 ; *JCP* 2000, éd. G., I. 199.
- note sous Cass. civ. 2e, 27 mai 1999, *JCP* 2000, éd. G., I. 197.
- note sous Cass. civ. 3e, 9 juill. 2003 et 3 déc. 2003, *JCP* 2004, éd. G., I. 163.

RAPPORTS, ETUDES, LIVRES BLANCS, GUIDES

ANTI-PHISHING WORKING GROUP
Phishing Activity Trends, août 2006, disponible sur :
http://www.antiphishing.org/reports/apwg_report_August_2006.pdf

ANZIANI (A.) et BETEILLE (L.) (présenté par)
Responsabilité civile : des évolutions nécessaires, Rapport d'information, Doc Sénat n° 558, 15 juill. 2009, spéc. p. 80, disponible sur : http://www.senat.fr/rap/r08-558/r08-5581.pdf

BITDEFENDER
Rapport sur l'état des e-menaces, 16 janvier 2009, disponible sur :
www.bitdefender.fr/site/News/pdfDescription/922.pdf)

BRAIBANT (G.)
Données personnelles et société de l'information : Transposition en droit français de la directive 95/46, Rapport au Premier ministre, Doc. fr., coll. *Rapports officiels*, Paris, 1998.

CNIL
- *Rapport d'activité* 1989, n° 10, Doc. fr., Paris, 1990.
- *Rapport d'activité 1996*, n° 17, Doc. fr., Paris, 1997.
- *Rapport d'activité* 1997, n° 18, Doc. fr., Paris, 1998.
- *Rapport d'activité 1998*, n° 19, Doc. fr., Paris, 1999.
- *Rapport d'activité 1999*, n° 20, Doc. fr., Paris, 2000.
- *Rapport d'activité 2001*, n° 22, Doc. fr., 2002.
- *Rapport d'activité 2003*, n° 24, Doc. fr. Paris, 2004.
- *Rapport d'activité 2005*, n° 26, Doc. fr., Paris, 2006.
- *Rapport d'activité 2006*, n° 27, Doc. fr., Paris, 2007.
- *Rapport d'activité 2009*, n° 30, Doc. fr., Paris, 2010.
- *Le publipostage électronique et la protection des données personnelles*, (Rapport présenté par Cécile ALVERGNAT), 14 octobre 1999, disponible sur :
http://www.cnil.fr/fileadmin/documents/approfondir/dossier/spam/boite_a_spam.pdf.
- *Opération " Boîte à spams " : Les enseignements et les actions de la CNIL en matière de communications électroniques non sollicitées*, (Rapport présenté par Cécile ALVERGNAT), 24 octobre 2002, disponible sur :
http://www.cnil.fr/fileadmin/documents/approfondir/rapport/boite_a_spam.pdf.
- *Internet et la collecte de données personnelles auprès des mineurs*, (Rapport présenté par Cécile ALVERGNAT), 12 juin 2001, disponible sur :
http://w3.scola.ac-paris.fr/juniors/droits/mineurs.pdf.
- Document d'orientation « pour la mise en œuvre de dispositifs d'alerte professionnelle conformes à la loi du 6 janvier 1978 modifiée en août 2004, relative à l'informatique, aux fichiers et aux libertés », 10 novembre 2005, disponible sur :
http://www.cnil.fr/fileadmin/documents/La_CNIL/actualite/CNIL-docori-10112005.pdf.
- « Guide droit d'accès », 2010, disponible sur :

http://www.cnil.fr/fileadmin/documents/Guides_pratiques/CNIL_Droit_d_acces.pdf.
- Guide « *La pub si je veux* », 2008, disponible sur :
http://www.cnil.fr/fileadmin/documents/Guides_pratiques/CNIL_Guide_pub.pdf
- Guide, « Transferts de données à caractère personnel vers des pays non membres de l'Union européenne », juin 2008, disponible sur :
http://www.cnil.fr/fileadmin/documents/approfondir/dossier/international/Guide-tranfertdedonnees.pdf.

CONSEIL NATIONAL DE LA CONSOMMATION
Rapport sur la protection des données personnelles des consommateurs, 18 mai 2010, disponible sur :
http://www.minefe.gouv.fr/directions_services/dgccrf/boccrf/2010/10_06/rapport_CNCdonnees_personnelles.pdf.

DETRAIGNE (Y.) ET ESCOFFIER (A.-M.) (présenté par)
Rapport d'information relatif au respect de la vie privée à l'heure des mémoires numériques, 27 mai 2009, Doc. Sénat n° 441, disponible sur : http://www.senat.fr/rap/r08-441/r08-4411.pdf.

DINANT (J.-M.)
Rapport sur les lacunes de la Convention n°108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel face aux développements technologiques (Partie I), Strasbourg, 22e réunion, novembre 2010, T-PD-BUR(2010)09 (I) FINAL, disponible sur :
http://www.coe.int/t/dghl/standardsetting/dataprotection/CoE%20Lacunes%20de%20la%20Convention%20108%20Part%20I%20TPD.pdf.

DINANT (J.-M.), LAZARO (C.), POULLET (Y.), et al. (rapport présenté par)
L'application de la Convention 108 au mécanisme de profilage : Éléments de réflexion destinés au travail futur du Comité consultatif, 24e réunion, 13-14 mars 2008, disponible sur :
http://www.coe.int/t/dghl/standardsetting/dataprotection/Reports/CRID_Profilage_2008_fr.pdf.

DIONIS DU SEJOUR (J.) ET (C.) ERHEL
Rapport d'information sur la mise en application de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, Doc A.N. n° 627, 23 janvier 2008, disponible sur :
http://www.assemblee-nationale.fr/13/pdf/rap-info/i0627.pdf.

ENISA
What are the Measures Used by European Providers to Reduce the Amount of Spam Received by Their Customers ?, décembre 2009, disponible sur :
http://www.enisa.europa.eu/act/res/other-areas/anti-spam-measures).

FTC
- *A CAN-SPAM Informant Reward System – A Report to Congress*, septembre 2004, disponible sur : http://www.ftc.gov/reports/rewardsys/040916rewardsysrpt.pdf.
- *Effectiveness and enforcement of CAN-SPAM Act – A Report of Congress*, décembre 2005, disponible sur : http://www.ftc.gov/reports/canspam05/051220canspamrpt.pdf.
- " How To Comply with the Privacy of Consumer Financial Information Rule of the Gramm-Leach-Bliley Act - A Guide for Small Business from the Federal Trade Commission ", juillet 2002, disponible sur : http://www.ftc.gov/bcp/edu/pubs/business/idtheft/bus67.shtm.
- *Label for E-mail Messages Containing Sexually Oriented Material*, 69 *C.F.R.* 21024, 19 avril 2004, disponible sur : http://www.ftc.gov/os/2004/04/040413adultemailfinalrule.pdf.
- *National Do Not Email Registry : A Report To Congress*, juin 2004, disponible sur :

http://www.ftc.gov/reports/dneregistry/report.pdf.
- *The CAN-SPAM Act : A Compliance Guide for Business*, septembre 2009, disponible sur : http://www.ftc.gov/bcp/edu/pubs/business/ecommerce/bus61.shtm.

GAUTHRONET (S.) et DROUARD (É.)
Communications commerciales non sollicités et données personnelles (Internal Market DG – Contract n° ETD/99/B5-3000/E/96), janv. 2001, disponible sur : http://www.rigacci.org/docs/biblio/online/spam_garante/document/434683.pdf.

IUT
Financial Aspects of Network Security: Malware and Spam, Final Report 2008, disponible sur : http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-study-financial-aspects-of-malware-and-spam.pdf).

MAILINBLACK
« *Spam* – État de l'art », Livre Blanc, 2006, disponible sur : http://assiste.com.free.fr/ftp/livre_blanc_le_*spam*.pdf.

MALCOLM HARBOUR (présenté par)
Rapport au nom de la Commission du marché intérieur et de la protection des consommateurs du 18 juillet 2008 sur la proposition de directive du Parlement européen et du Conseil modifiant notamment la directive 2002/58/CE (2007/0248(COD)), A6-0318/2008, disponible sur : http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+CRE+20080902+ITEM-010+DOC+XML+V0//FR).

OCDE
- *Document exploratoire sur le vol d'identité en ligne*, DSTI/CP(2007)/3/FINAL, Séoul Corée, 17–18 juin 2008, disponible sur : http://www.oecd.org/dataoecd/3/8/40699509.pdf.
- *Le commerce mobile*, DSTI/CP(2006)7/FINAL, 9 févr. 2007, disponible sur : http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/CP(2006)7/FINAL&docLanguage=Fr.
- *Les logiciels malveillants (maliciels) : Une menace à la sécurité de l'économie de l'Internet*, DSTI/ICCP/REG(2007)5/FINAL, 27 mai 2008, disponible sur : http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP/REG%282007%295/FINAL&docLanguage=Fr.
- *Rapport du Groupe de réflexion sur le spam de l'OCDE : Boîte à outils anti-spam de politiques et mesures recommandées*, DSTI/CP/ICCP/*SPAM*(2005)3/FINAL, 19 mai 2006, disponible sur : http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/CP/ICCP/SPAM(2005)3/FINAL&docLanguage=Fr.

SOPHOS
- « Classement trimestriel des douze principaux pays relayeurs de *spam* : la France premier émetteur européen », 14 oct. 2010, disponible sur : http://www.sophos.fr/pressoffice/news/articles/2010/10/dirty-dozen-q32010.html.
- « Les virus et le *spam*, ce qu'il faut savoir », disponible sur : http://mirror.sweon.net/madchat/vxdevl/library/Les%20virus%20et%20le%20*spam*%20-%20ce%20qu%27il%20faut%20savoir.pdf.
- *Rapport sur les menaces à la sécurité*, 2010, disponible sur : http://www.sophos.fr/sophos/docs/fra/papers/sophos-security-threat-report-jan-2010-wpfr.pdf.
- *Security threat Report*, 2009, disponible sur :

http://www.sophos.com/sophos/docs/eng/marketing_material/sophos-security-threat-report-jan-2009-na.pdf.
- *Security Threat Report*, 2011, disponible sur:
http://www.sophos.com/en-us/press-office/press-releases/2011/01/threat-report-2011.aspx.
- " The *spam* economy: the convergence *spam* and virus threats ", mai 2005, disponible sur :
http://www.sophos.com/whitepapers/Sophos_*spam*-economy_wpus.pdf.

SYMANTEC
" State of Spam and Phishing ", n° 47, nov. 2010, disponible sur :
http://www.symantec.com/content/en/us/enterprise/other_resources/b-state_of_spam_and_phishing_report_11-2010.en-us.pdf).

US DEPARTMENT OF HOMELAND
The Crimeware Landscape : Malware, Phishing, Identity Theft and Beyond, octobre 2006, disponible sur : http://www.antiphishing.org/reports/APWG_CrimewareReport.pdf

COMMUNICATIONS, COMMUNIQUES DE PRESSE, CONFERENCE, COLLOQUE

BITDEFENDER
- Communiqué de presse, 8 avril 2008, disponible sur :
http://www.editions-profil.eu/EP/RessourcesSiteProfil/Communiques/Alerte%20du%20080408.pdf.
- Communiqué de presse, 24 août 2010, disponible sur :
http://www.editions-profil.eu/EP/RessourcesSiteProfil/Communiques/Rapport%20BitDefender%20sur%20l%E2%80%99%C3%A9tat%20des%20e-menaces%20au%20premier%20semestre%202010.pdf.
- Communiqué de presse, 9 oct. 2008, disponible sur :
http://www.editions-profil.eu/EP/RessourcesSiteProfil/Communiques/BitDefender%20et%20la%20technique%20des%20*spams*.pdf.

CNIL (organisée par)
23e conférence internationale des commissaires à la protection des données : *Vie privée – Droits de l'homme,* 24-26 sept. 2001, Doc. fr., 2002.

COMMISSION EUROPEENNE
- « Approche globale de la protection des données à carcatère personnel dans l'Union européenne », Bruxelles, 4 novembre 2010, COM(2010) 609 final, disponible sur : http://ec.europa.eu/health/data_collection/docs/com_2010_0609_fr.pdf.

Communication de la Commission au Parlement européen, au Conseil, Comité économique et social européen et au Comité des régions, Évaluation finale de la mise en œuvre du programme communautaire pluriannuel visant à promouvoir une utilisation plus sûre de l'internet et des nouvelles technologies en ligne, 18 févr. 2009, COM/2009/0064/final, disponible sur :
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52009DC0064:FR:NOT

INNES-STUBB (S.) ET GELLMAN (R.)
« L'approche américaine : la régulation par le congrès, le marché et le juge » *in Informatique : servitude ou libertés ?*, Colloque organisé par la CNIL et l'université Panthéon-Assas-Paris II, Sénat, 7 et 8 nov. 2005, disponible sur :
http://www.senat.fr/colloques/colloque_cnil_senat/colloque_cnil_senat.html.

NOVELLI (H.)
« Lutter contre les *spams* par SMS et vocaux et les prospections téléphoniques non désirées », communiqué de presse, 21 juin 2010, disponible sur : http://www.economie.gouv.fr/presse/dossiers_de_presse/100621spam.pdf).

STEEVES (V.)
« La protection en ligne de la vie privée des enfants », *in* 29e Conférence des Commissaires à la protection des données et de la vie privée, 27 septembre 2007, disponible sur : http://www.privacyconference2007.gc.ca/workbooks/Terra_Incognita_workbook10_bil.pdf.

RECOMMANDATIONS, AVIS, DELIBERATIONS, DECISIONS, PROPOSITIONS DE REGLEMENT

A.R.T
Avis no 2001-423 du 2 mai 2001 sur le projet de loi sur la société de l'information.

CNIL
- Avis sur le projet de loi modifiant la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, 26 septembre 2000, disponible sur : http://www.cnil.fr/fileadmin/documents/approfondir/textes/aviscnildonneesperso.pdf.
- Délibération n° 88-052 du 10 mai 1988 portant adoption d'une recommandation sur la compatibilité entre les lois n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, et n° 79-18 du 3 janvier 1979 sur les archives.
- Délibération n° 02-074 du 24 octobre 2002 portant adoption du rapport relatif à l'opération " Boîte à *spams* " *in Rapport d'activité 2002*, n° 23, Doc. fr., 2003, spéc. p. 224.
- Délibération n° 01-057 du 29 novembre 2001 portant recommandation sur la diffusion de données personnelles sur internet par les banques de données de jurisprudence.
- Délibérations n° 02-075 (concernant la Société ABS), n° 02-076 du 24 octobre 2002 (concernant la Société BV COMMUNICATION), n° 02-077 (concernant la Société GREAT-MEDS.COM), n° 02-078 (concernant la Société SUNILES), n° 02-079 (concernant une lettre le Top 50 des sites X) du 24 octobre 2002 portant dénonciation au Parquet d'infractions à la loi du 6 janvier 1978, *in Rapport d'activité 2002*, rapport préc., spéc. p. 225 et s.
- Délibération n° 02-093 du 28 novembre 2002 portant avis sur le projet de loi relatif à l'économie numérique *in* CNIL, *Rapport d'activité 2002*, rapport préc., spéc. p. 180.
- Délibération n° 2006-147 du 23 mai 2003 fixant le règlement intérieur de la CNIL, J.O. du 7 juillet 2006, n° 156.
- Délibération n° 2005-112 du 07 juin 2005 portant création d'une norme simplifiée concernant les traitements automatisés de données à caractère personnel relatifs à la gestion des fichiers de clients et de prospects et portant abrogation des normes simplifiées 11, 17 et 25, disponible sur : http://www.cnil.fr/en-savoir-plus/deliberations/deliberation/delib/184/.
- Délibération n° 2006-228 du 5 octobre 2006 portant recommandation relative à la mise en œuvre par les partis ou groupements à caractère politique, élus ou candidats à des fonctions électives de fichiers dans le cadre de leurs activités politiques, disponible sur : http://www.cnil.fr/en-savoir-plus/deliberations/deliberation/delib/114)/.
- Délibération n° 2006-294 du 21 déc. 2006 autorisant la mise en œuvre par l'Association de Lutte contre la Piraterie Audiovisuelle (LPA) d'un traitement de données à caractère personnel ayant pour finalité principale la recherche des auteurs de contrefaçons audiovisuelles.
- Délibération n° 2007-049 du 15 mars 2007 sanctionnant la société STUDIO REPLAY, disponible sur : http://www.cnil.fr/en-savoir-plus/deliberations/deliberation/delib/152/
- Délibération n° 2008-163 du 12 juin 2008 prononçant une sanction pécuniaire à l'encontre de la société NEUF CEGETEL, disponible sur : http://www.cnil.fr/en-savoir-plus/deliberations/deliberation/delib/149/.

- Délibération n° 2008-422 du 6 novembre 2008 portant décision de la formation restreinte à l'égard de la société CDISCOUNT, disponible sur :
http://www.cnil.fr/en-savoir-plus/deliberations/deliberation/delib/147/.
- Délibération n° 2008-470 du 27 novembre 2008 de la formation restreinte prononçant une sanction pécuniaire à l'encontre de la société ISOTHERM, disponible sur :
http://www.cnil.fr/en-savoir-plus/deliberations/deliberation/delib/204/.
- Délibération n° 2010-232 du 17 juin 2010 de la formation restreinte prononçant une sanction pécuniaire à l'encontre de la société JPSM, disponible sur :
http://www.cnil.fr/en-savoir-plus/deliberations/deliberation/delib/248/.

COMITE DES MINISTRES AUX ÉTATS MEMBRES SUR LA PROTECTION DE LA VIE PRIVEE SUR INTERNET

Recommandation n° R (99) 5, « *Lignes Protectrices pour la protection des personnes à l'égard de la collecte et du traitement de données à caractère personnel sur les "inforoutes"* », 23 février 1999, disponible sur :
https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=276586&SecMode=1&DocId=396770&Usage=2.

CONSEIL CONSTITUTIONNEL

- DC n° 84-181 du 11 octobre 1984, J.O. du 29 juillet 1984, p. 3200 et s., *Rec. const.*, p. 78
- Dc n° 89-257 du 25 juillet 1989, J.O. du 28 juillet 1989, p. 9503 et s., *Rec. constit*., p. 59.
- Dc n° 89-260 du 28 juillet 1989, J.O. du 1er août 1989, p. 9676 et s., *Rec. const*., p. 71.
- DC n° 2004-499 du 29 juill. 2004, J.O. du 7 août 2004, p. 14087, *Rec. const*., p. 126 ; *Comm. com. électr*. nov. 2004, comm. 146, p. 35 et s., note A. Lepage.
- DC n° 2009-580 du 10 juin 2009, J.O. du 13 juin 2009, p. 9675 ; *Rec. const*., p. 107.

CONTROLEUR EUROPEEN DE LA PROTECTION DES DONNEES

- Avis sur la proposition de directive du Parlement européen et du Conseil modifiant, entre autres, la directive 2002/58/CE, J.O.U.E. n° C 181 du 18 juillet 2008, p. 1 et s., disponible sur :
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2008:181:0001:0001:FR:PDF.
- Deuxième avis relatif au réexamen de la directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive « vie privée et communications électroniques ») du 9 janvier 2009, J.O.U.E.. n° C. 128 du 6 juin 2009, p. 28 et s., disponible sur :
http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2009/09-01-09_ePricacy_2_FR.pdf

FTC

- *Definitions, Implementation, and Reporting Requirements Under the CAN-SPAM Act"*, Proposed Rule, 70 *F.R.* 25426, 12 mai 2005, disponible sur :
http://www.ftc.gov/os/2005/05/05canspamregformfrn.pdf.
- *Definitions, Implementation, and Reporting Requirements Under the Can-Spam Act"*, Final Rule, 73 *F.R* 29654, 16 *C.F.R.* Part 316, 21 mai 2008, disponible sur :
http://www.ftc.gov/os/2008/05/R411008frn.pdf.
- A Brief Overview of the Federal Trade Commission's Investigative and Law Enforcement Authority, juillet 2008, disponible sur : http://www.ftc.gov/ogc/brfovrvw.shtm.

GROUPE « ARTICLE 29 »

- Avis n° 5/2004 portant sur les communications de prospection directe non sollicitées selon l'article 13 de la directive 2002/58/CE, 11601/FR, WP 90, 27 février 2004, disponible sur :
http://www.cnpd.public.lu/fr/publications/groupe-art29/wp090_fr.pdf.
- Avis n° 4/2007 sur le concept de données à caractère personnel, 01248/07/FR, WP 136, 20 juin 2007, disponible sur :

http://www.cnpd.public.lu/fr/publications/groupe-art29/wp136_fr.pdf.
- Avis n° 1/2008 sur les aspects de la protection des données liés aux moteurs de recherche, 00737/FR,WP 148, 4 avril 2008, disponible sur :
http://www.cnil.fr/fileadmin/documents/approfondir/dossier/internet/wp148_fr.pdf.
- Avis n° 2/2008 sur la révision de la directive 2002/58/CE, 00989/08/FR, WP 150, 15 mai 2008, spéc. p. 3, disponible sur :
http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp150_fr.pdf.
- Avis n° 1/2010 sur les notions de « responsable du traitement » et de « sous-traitant », 16 février 2010, 00264/10/FR, WP 169, disponible sur :
http://www.cnpd.public.lu/fr/publications/groupe-art29/wp169_fr.pdf.
Avis n° 2/2010 sur la publicité comportementale en ligne, 00909/10/FR, WP 171, 22 juin 2010, disponible sur :
http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_fr.pdf.

TEXTES NORMATIFS

Français et européens

LOIS

Loi de finances n° 63-628 du 2 juillet 1963 rectificative pour 1963 portant maintien de la stabilité économique et financière, J.O. du 3 juillet 1963, p. 5915 et s.

Loi n° 73-1193 du 27 décembre 1973, d'orientation, du commerce et de l'artisanat, dite « loi Royer », J.O. du 30 décembre 1973, p. 14139 et s.

Loi n° 78-17 du 6 janvier 1978 relative à l'Informatique, aux fichiers et aux Libertés, J.O. du 7 janvier 1978, p. 227 et s. et rectificatif, J.O. du 25 janvier 1978.

Loi n° 88-19 du du 5 janvier 1988 sur la fraude informatique, J.O. du 6 janvier 1988, p. 231 et s.

Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, J.O. n° 143 du 22 juin 2004, p. 1168 et s.

Loi n° 2004-669 du 9 juillet 2004 relative aux communications électroniques et aux services de communication audiovisuelle, J.O. n° 159 du10 juillet 2004, p. 12483 et s.

Loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, J.O. n° 182 du 7 août 2004, p. 14063 et s.

Loi n° 2008-3 du 3 janvier 2008 pour le développement de la concurrence au service des consommateurs, dite « loi Chatel », J.O. du 4 janvier 2008, p. 258 et s.

Loi n° 2008-776 du 4 août 2008 de modernisation de l'économie, dite « loi LME », J.O. du 5 août 2008, p. 12471 et s.

Loi n° 2011-267 du 14 mars 2011d'orientation et de programmation pour la performance de la sécurité intérieure du 14 mars 2011, J.O. du 15 mars 2011, p. 4582 et s.

PROPOSITIONS ET PROJETS DE LOI

BETEILLE (L.) (présentée par)
Proposition de loi portant réforme de la responsabilité civile, Doc Sénat n° 657, 9 juillet 2010, disponible sur : http://www.senat.fr/leg/ppl09-657.pdf.

CATALA (P.) (sous la dir.)
Avant-projet de réforme du droit des obligations et de la prescription, dit « projet CATALA », rapport au garde des Sceaux, 22 sept. 2005, Doc. fr. 2006.

DETRAIGNE (Y.) et ESCOFFIER (A.-M.) (présentée par)
Proposition de loi visant à mieux garantir le droit à la vie privée à l'heure du numérique, Doc. Sénat n° 93, enregistrée le 6 novembre 2009, disponible sur : http://www.senat.fr/leg/ppl09-093.pdf.

FABIUS (L.) (présenté par)
Projet de loi sur la société de l'information, enregistré le 14 juin 2001, Doc. A.N. n° 3143, disponible sur http://www.assemblee-nationale.fr/11/projets/pl3143.asp.

Projet de loi portant diverses dispositions d'adaptation de la législation au droit de l'Union européennes en matière de santé, de travail et de communications électroniques, Étude d'impact, Doc. A. N. n° 225, enregistré le 14 septembre 2010, disponible sur : http://www.senat.fr/leg/pjl10-225.pdf.

ORDONNANCES

Ordonnance n° 2001-670 du 25 juillet 2001 portant adaptation au droit communautaire du Code de la propriété intellectuelle et du Code des postes et télécommunications, J.O. n° 173 du 28 juillet 2001, p. 12132 et s.

Ordonnance n° 2001-741 du 23 août 2001 portant transposition des directives communautaires et adaptation au droit communautaire en matière de droit de la consommation, J.O. n° 196 du 25 août 2001, p. 13645 et s.

REGLEMENTS ET PROPOSITIONS DE REGLEMENTS, RESOLUTIONS

Règl. (CE) n° 44/2001 du Conseil du 22 décembre 2000 concernant la compétence judiciaire, la reconnaissance et l'exécution des décisions en matière civile et commerciale, J.O.U.E. n° L. 12 du 16 janvier 2001, p. 1 et s.

Proposition de règlement du Parlement européen et du Conseil sur la loi applicable aux obligations non contractuelles, 22 juillet 2003, COM (2003) 427 final.

Règl. (CE) n° 460/2004 du Parlement européen et du Conseil du 10 mars 2004 instituant l'Agence européenne chargée de la sécurité des réseaux et de l'information, J.O.U.E. n° L 77 du13 mars 2004, p. 1 et s.

Règl. (CE) n° 864/2007 du Parlement européen et du Conseil sur la loi applicable aux obligations non contractuelles du 11 juillet 2007, J.O.U.E. n° L 199 du 31 juillet 2007, p. 40 et s.

PARLEMENT EUROPÉEN
Resolution on the implementation and review of Council Regulation (EC) n° 44/2001 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters, 2009/2140 (INI), du 7 septembre 2010.

Proposition de règlement du Parlement européen et du Conseil concernant la compétence judiciaire, la reconnaissance et l'exécution des décisions en matière civile et commerciale (Refonte), 14 décembre 2010, COM(2010) 748 final, 2010/0383 (COD).

DECRETS

Décret n° 2005-1309 du 20 octobre 2005 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

Décret n° 2005-605 du 27 mai 2005 modifiant la deuxième partie du CPCE, J.O. n° 124 du 29 mai 2005.

Décret n° 2005-606 du 27 mai 2005 relatif aux annuaires et aux services de renseignements et modifiant le CPCE, J.O. n° 124 du 29 mai 2005.

Décret n° 2007-451 du 25 mars 2007 modifiant le décret du 20 octobre 2005 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2004-801 du 6 août 2004.

DIRECTIVES

Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, J.O.U.E. n° L.281 du 23 novembre 1995, p. 31 et s.

Directive 97/7/CE du Parlement européen et du conseil du 20 mai 1997 concernant la protection des consommateurs en matière de contrats à distance, J.O.U.E. n° L. 144 du 4 juin 1997, p. 19 et s.

Directive 97/66/ CE du Parlement européen et du Conseil du 15 décembre 1997 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications, J.O.U.E. n° L. 24 du 30 janvier 1998, p. 1 et s.

Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur, J.O.U.E. n° L. 178 du 17 juillet 2000, p. 1 et s.

Directive 2002/58/ CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques), J.O.U.E. n° L. 201 du 31 juillet 2002, p. 37 et s.

Directive n° 2005/29/CE du Parlement européen et du Conseil du 11 mai 2005 relative aux pratiques commerciales déloyales des entreprises vis-à-vis des consommateurs dans le marché intérieur et modifiant la directive n° 84/450/CE du Conseil et les directives n° 97/27/CE,

98/27/CE et 2002/65/CE du Parlement européen et du conseil et le règlement (CE) n° 2006/2004 du Parlement européen et du Conseil, J.O.U.E. n° L 149/22 du 11 juin 2005, p. 22 et s.

Directive 2009/136/CE du Parlement européen et du Conseil du 25 novembre 2009 modifiant la directive 2002/22/Ce concernant le service universel et les droits des utilsateurs au regard des réseaux et des services de communications, la directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques et le règlement (CE) n° 2006/2004 relatif à la coopération entre les autorités nationales chargées de veiller à l'application de la législation en matière de protection des consommateurs, J.O.U.E. n° L. 337 du 18 décembre 2009, p. 11 et s.

CONVENTIONS

Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, *S.T.E.* n° 108, Strasbourg, 28 janvier 1981, J.O. du 20 novembre 1985, p. 13436 et s.).

Convention de Rome de 1980 sur la loi applicable aux obligations contractuelles (version consolidée), J.O.U.E. C. 27 du 26 janvier 1998, p. 34 et s.

Américains

LOIS

Children's Online Privacy Protection Act (COPPA) (15 *U.S.C.* 6501-6506)

Controlling the Assault of Non-Sollicited Pornographie and Marketing (*CAN-SPAM Act*), 108th Congress, Pub. L. n° 108-187, Sec. 2, 117 Stat. 2699 (16 déc. 2003), 15 *U.S.C.* Sec. 7701-7713 et 18 *U.S.C.* Sec. 1037, disponible sur :
http://uscode.house.gov/download/pls/15C103.txt.

Telephone Consumer Protection Act of 1991.

The Financial Modernization Act (15 *U.S.C.* 6801-6809).

Fair Credit Reporting Act (FCRA) (15 *U.S.C.* 1681 et seq.).

Health Insurance Portability and Accountability Act (HIPPA) (42 *U.S.C.* Sec. 201 et seq.)

PROPOSITIONS DE LOIS

Data Privacy Act of 1997 (H.R. 2368, 105th Cong.).
Unsolicited Commercial Electronic Mail Choice Act of 1997 (S. 771, 105th Cong.).
Electronic Mailbox Protection Act of 1997 (S. 875, 105th Cong.).
Nitizens Protection Act (H.R. 1748, 105th Cong.).
E-Mail User Protection Act of 1998 (H.R. 4124, 105th Cong.).
Anti-Slamming Amendmends Act of 1998 (S. 1618, 105th Cong.).
Digital Jamming Act of 1998 (H.R. 4176, 105th Cong.).

Inbox Privacy Act of 1999 (S. 759, 106th Cong.)
Internet Growth and Development Act of 1999 (H.R. 1685, 106th Cong.).
Internet Freedom Act (H.R. 1686, 106th Cong.).
E-Mail User Protection Act (H.R. 1910, 106th Cong.).
Protection Against Scams on Seniors Act of 1999 (H.R. 612, 106th Cong.).
Telemarketing Fraud and Seniors Protection Act (S. 699, 106th Cong.).
Netizens Protection Act of 1999 (H.R. 3024, 106th Cong.).
Wireless Telephone Spam Protection Act (H.R. 5300, 106th Cong.).
CAN-SPAM Act (H.R. 2162, 106th Cong.).
Unsolicited Commercial Electronic Mail Act of 2000 (H.R. 3113, 106th Cong.).
Controlling the Assault of Non-Solicited Pornography and Marketing (CAN SPAM) *Act of 2000* (S. 2542, 106th Cong.).

Anti-Spamming Act of 2001 (H.R. 1017, 107th Congr.).
*Controlling the Assault of Non-Solicited Pornography and Marketing (*CAN SPAM*) Act of 2001/2002* (S. 630, 107th Congr.).
Netizens Protection Act of 2001 (H.R. 3146, 107th Congr.).
Protection Children From E-Mail Smut Act of 2001 (H.R. 2472, 107th Congr.).
Who Is E-Mailing Our Kids Act (H.R. 1846, 107th Congr.).
Unsolicited Commercial Electronic Mail Act of 2001 (H.R. 95, 107th Congr.).
Wireless Telephone Spam Protection Act (H.R. 113, 107th Congr.).

Anti-Spam Act of 2003 (H.R. 2515, 108th Cong.).
Criminal Spam Act of 2003 (S. 1293, 108th Cong.).
Wireless Telephone Spam Protection Act (H.R. 122, 108th Cong.).
REDUCE Spam Act (*Restrict and Eliminate the Delivery of Unsolicited Commercial Electronic Mail or Spam Act of* 2003 (H.R. 1933, 108th Cong.).
Stop Pornography and Abusive Marketing Act (S. 1231, 108th Cong.).
Ban on Deceptive Unsolicited Bulk Electronic Mail Act of 2003 (S. 1052, 108th Cong.).
Computer Owner's Bill of Rights (S. 563, 108th Cong.).
Reduction in Distribution of Spam Act of 2003 (H.R. 2214, 108th Cong.).

Privacy Act (S. 116, 109th Congress, Session 1st, 2005).
Personal Data Privacy and Security Act of 2005 (S. 1332, 109th Congress, Session 1st, 2005).
Personal Data Privacy and Security Act of 2009 (S. 1490, 111th Congress, 1st Session, 2009*).*

RESSOURCES ELECTRONIQUES

SITES *WEB* INSTITUTIONNELS ET ADMINISTRATIFS

http://www.afa-france.com.
http://www.caspam.org.
http://www.cnpd.public.lu/fr/index.html.
http://www.cnil.fr.
http://www.coppa.org/.
http://www.ddm.gouv.fr.
http://www.economie.gouv.fr.
http://www.euroispa.org.
http://www.enisa.europa.eu.
http://europa.eu

http://www.federalregister.gov. .
http://www.foruminternet.org.
http://www.ftc.gov.
http://www.hhs.gov/ocr/privacy/.
http://www.icc-cpi.int/.
http://www.interieur.gouv.fr.
http://www.londonactionplan.com.
http://www.maawg.org.
http://www.oecd.org.
http://www.spamhaus.org.
http://www.telecom.gouv.fr.
http://thomas.loc.gov/.
http://www.wto.org.

AUTRES SITES

http://www.33700-spam-sms.fr/.
http://www.altospam.com/fr/societe.php.
http://www.arobase.org.
http://assiste.com.free.fr.
http://row.avira.com.
http://www.globalsecuritymag.fr.
http://www.microsoft.com.
http://netiquette.fr/
http://networketiquette.net/
http://www.rfc1855.net/
http://www.spamlaws.com.
http://www.securelist.com.
http://www.securiteinfo.com/
http://www.stopmessengerspam.com/.
http://www.symantec.com.
http://www.usenet-fr.net.

ARTICLES DE PRESSE ET ARTICLES NON JURIDIQUES

ALTOSPAM
« Les conséquences du *spamming* », actualité 2009, disponible sur :
http://www.altospam.com/actualite/2009/06/les-couts-economiques-du-spamming/

BOUCHER (P.)
« Safari ou la chasse aux français », Le Monde, 21 mars 1974, p. 9, disponible sur :
http://rewriting.net/wp-content/le_monde_-_21_03_1974_009-3.jpg.

CAPELLI (P.)
« Les nouveaux explorateurs du continent numérique », 4 févr. 2010**,** disponible sur :
http://www.strategies.fr/actualites/marques/131963W/les-nouveaux-explorateurs-du-continent-numerique.html).

CHASTANT (J. -B.)
« La délicate question du droit à l'oubli sur Internet », 12 nov. 2009, disponible sur :

http://www.lemonde.fr/technologies/article/2009/11/12/la-delicate-question-du-droit-a-l-oubli-sur-internet_1266457_651865.html

FERRAN (B.)
« Une faille de *Twitter* utilisée pour propager du *spam* », 21 septembre 2010, disponible sur : http://www.lefigaro.fr.

GROS (M.)
« Nathalie KOSCIUSKO-MORIZET veut concrétiser le droit à l'oubli », 12 nov. 2009, disponible sur : http://www.lemondeinformatique.fr/actualites/lire-nathalie-kosciusko-morizet-veut-concretiser-le-droit-a-l-oubli-numerique-29416-page-2.html.

LEWIS (D.)
" The recent drop in global spam volumes – what happened ", 6 octobre 2010, disponible sur : http://www.symantec.com/connect/blogs/recent-drop-global-spam-volumes-what-happened.

MCCULLAGH (D.)
" LexisNexis flap draws outcry from Congress ", 12 avril 2005, disponible sur : http://news.cnet.com/LexisNexis-flap-draws-outcry-from-Congress/2100-7348_3-5668119.html?tag=mncol;txt et les différents liens).

« Marionnaud au parfum *Bluetooth* », 31 mai 2007, disponible sur : http://www.strategies.fr/actualites/marques/r44927W/marionnaud-au-parfum-bluetooth.html.

NAMESTNIKOV (Y.)
" The economics of botnet ", 2009, disponible sur : http://www.securelist.com/en/downloads/pdf/ynam_botnets_0907_en.pdf.

SANTROT (F.)
« Le " spam-up ", nouvelle plaie du Web », 21 juill. 2003, disponible sur : http://www.journaldunet.com/0307/030721spamup.shtml.

SOPHOS
- « Classement trimestriel des douze pays relayeurs de *spam* », 14 oct. 2010, disponible sur : http://www.sophos.fr/pressoffice/news/articles/2010/10/dirty-dozen-q32010.html.
- " The top twelve spam relaying countries for october – December 2010 ", 11 janv. 2011, disponible sur : http://www.sophos.com/en-us/press-office/press-releases/2011/01/dirty-dozen-q42010.aspx.
- « Une nouvelle escroquerie sur Facebook propose un faux bouton "Je n'aime pas" », 16 août 2010, disponible sur : http://www.sophos.fr/pressoffice/news/articles/2010/08/facebook-dislike.html.

THE SPAMHAUS PROJECT
" The 10 Worst Spammers" , 6 mai 2011, disponible sur : http://www.spamhaus.org/statistics/spammers.lasso.

VADE RETRO TECHNOLOGY
« Calculateur du coût du *spam* », disponible sur : http://www.antispam.fr/fr/spam_calculator.asp).

VERJUS (L.)
« Le *spamming* en question : Exemples illustrés et conseils pratiques », nov. 2006, disponible sur : http://statbel.fgov.be/fr/binaries/spamming_in_question_fr_tcm326-42567.pdf.

YAHOO! « Prouver et sécuriser l'identité des expéditeurs », disponible sur : http://fr.docs.yahoo.com/mail/spamguard_domainkeys.html.

YAHOO! Media Relations
« *Sendmail* and Yahoo ! Mail collaborate to develop and deploy Domainkeys », disponible sur : http://docs.yahoo.com/docs/pr/release1143.html.

GLOSSAIRE

- A -

- **Administrateur de zombies** : personne qui contrôle à distance des réseaux de PC zombies.

- **Adresse électronique :** chaîne de caractères permettant de s'identifier et d'accéder à sa messagerie électronique afin d'envoyer et de recevoir du courrier électronique.

- **Adresse Ip** : série de chiffres permettant d'identifier un ordinateur ou un serveur.

- **Adresse MAC** ***(****Media Access Control address)* : numéro unique stocké dans une carte réseau permettant de l'identifier et ainsi d'attribuer mondialement une adresse unique au niveau de la couche de liaison.

- **Annuaire d'adresses :** bibliothèque électronique contenant certaines informations telles des noms et adresses électroniques.

- **Anonymiseurs *(Remailer)* :** Système qui permet à un internaute de naviguer sur l'internet de façon anonyme.

- **Anti-*spam*** : de nature à combattre le *spamming* et permet de qualifier ainsi des logiciels, des filtres, etc.

- **Appairage :** technique informatique utilisée afin de permettre une connexion entre les appareils. L'utilisation la plus courante est l'appairage d'un équipement *Bluetooth* avec une base *Bluetooth*.

- **ARCII Art (*American Standard Code for Information Interchange*) :** Code américain apparu dans les années 60 pour répondre aux besoins de trouver de nouveaux codes de communication plus riches et fonctionnels que les codes Morse ou Baudot.

- **Attaque DHA (*Directory Harvest Attack*)** : piratage d'annuaires qui consiste à reconstituer des adresses électroniques à partir d'une combinaison classique associant ses nom et prénom.

- **Authentification :** Moyen de vérification de la source d'un *e-mail*.

- B -

- ***Backdoor*** : porte dérobée.

- **Bande passante :** Capacité d'un réseau à transmettre un volume d'informations entre un serveur et un poste client. La vitesse de connexion à l'internet dépend de la bande passante du FAI.

- ***Blacklist*** (v. Liste noire)

- **Blog** : journal personnel qui permet à un internaute de publier régulièrement des informations ou de commenter l'actualité sur un sujet.

- ***Blue spam :*** nouvelle forme de *spam* qui se répand *via* le réseau *Bluetooth.*

- ***Bluetooth :*** technologie utilisant une technique radio courte distance permettant de faire communiquer entre eux divers appareils électroniques.

- C -

- C**haîne de courriers électroniques (*hoax*) :** canulars, mauvaises blagues informatiques envoyés par courrier électronique, faisant croire aux destinataires qu'ils proviennent d'expéditeurs connus de ces derniers.

- C**hamp CCI :** Signifie « Copie conforme invisible », et s'analyse en une option utilisée dans la phase d'envoi de courriers électroniques, permettant d'ajouter un ou plusieurs destinataires, sans qu'ils ne puissent s'identifier entre eux.

- Cheval de Troie : programme qui réalise une tâche à l'insu de l'utilisateur. À la différence du virus, il ne se reproduit pas mais peut être diffusé par des virus sur l'ordinateur qu'ils infectent.

- ***Cookies* :** fichiers stockés sur l'ordinateur d'un internaute par l'administrateur du site *Web* consulté permettant de mémoriser les données relatives à sa navigation et de faciliter ainsi les prochaines consultations de ce site

- **Courrier électronique (*e-mail*)** : service de transmission de messages échangés entre des utilisateurs via un réseau informatique, dans la boîte aux lettres électronique d'un destinataire choisi par l'émetteur.

- C**ryptographie** : ensemble des principes, méthodes et techniques dont l'application assure le chiffrement des données afin d'en préserver la confidentialité et l'authenticité.

- D -

- **Défaçage** : modification par une personne non autorisée de la page d'accueil d'un site *Web*.

- **DNS** (*Domain Name System*) : logiciel qui fait la conversion entre les adresses IP et les noms de domaine.

- **Domaine** (nom de domaine) : identifiant unique attribué à une entité dont les postes informatiques sont reliés à l'internet.

- ***Domain Keys Identified Mail* (DKIM) :** procédure d'authentification du nom de domaine de l'expéditeur d'un courrier électronique.

- E -

- Escroquerie à la nigériane : S'inspirant d'une escroquerie très ancienne, le « spammeur » envoie un message dans lequel il se présente comme l'héritier d'un riche notable africain récemment décédé et prétexte que ce dernier aurait déposé, à son intention, des millions de dollars sur un compte bancaire. Pour procéder au transfert de ces fonds, le « spammeur » s'en remet alors aux services du destinataire du message en le persuadant qu'il a besoin des coordonnées de son compte bancaire pour procéder au virement en échange d'un pourcentage substantiel sur cette somme.

- F -

- **Faux négatif** : erreur d'identification réalisée par le logiciel anti-*spam* se traduisant par le classement à tort de *spams* comme messages légitimes.

- **Faux positif** : erreur d'identification réalisée par le logiciel anti-*spam* se traduisant par le classement à tort de messages légitimes comme *spams*.

- **Filtrage Bayesien:** filtrage anti-*spam* dont le fonctionnement est inspiré de la théorie statistique mise au point au XVIII^{e} siècle par un pasteur et mathématicien britannique, Thomas BAYES, qui a été par la suite utilisée pour détecter si un courrier électronique était du *spam.*

- **FAI (**Fournisseur d'Accès à Internet) : prestataire de service qui offre à ses clients un accès au réseau Internet.

- **Forum de discussion (*newsgroup*) :** Pages de sites internet sur lesquelles des internautes discutent en échangeant des messages autour d'un sujet donné.

- **Fournisseurs de messagerie :** Prestataire de service qui fournit à ses clients une adresse électronique afin d'envoyer et de recevoir des *e-mails*.

- G -

- **Gardien de zombies (***bot herder*) : personne qui contrôle à distance des réseaux de PC zombies.

- H -

- ***Hashbusting*** : vise à créer des textes dynamiques en introduisant de légères variations dans le *spam* originel afin de masquer la similarité des contenus envoyés.

- ***Harvesting*** : collecter massivement des adresses électroniques présentes dans les espaces publics de l'internet.

- ***Hoax*** (v. chaînes de courriers électroniques)

- ***HoneyPot*** (v. Pot de miel).

- I -

- **Identifiant *Bluetooth* :** données permettant à un internaute de s'identifier auprès d'une connexion *Bluetooth*.

- **Ingénierie sociale** (*social engineering*) : recouvre différentes techniques destinées à tromper une personne afin d'amener cette dernière à fournir des informations ou à réaliser une opération permettant d'infiltrer la sécurité des systèmes d'information.

- **Internet:** réseau informatique mondial reposant sur le système d'adresses global des protocoles de communication TCP/IP (Transmission Control Protocol/Internet Protocol) et qui rend accessible des services comme par exemple, le courrier électronique.

- **IP (*Internet Protocol*) :** protocole Internet qui gère le transport et le routage des paquets sur le réseau.

- K –

- ***keywords stuffing:*** bourrage de mots-clés.

- L -

- **Lettre d'information (*newsletter*) :** lettre adressée de manière régulière par courrier électronique à des internautes qui s'y sont au préalable inscrits.

- **Liste blanche (*whitelist*)** : liste regroupant les noms de domaines, adresses électroniques et d'adresses Ip d'expéditeurs identifiés comme fiables.

- **Liste de diffusion (*Mailing list*)** : Système d'utilisation spécifique du courrier électronique qui permet le publipostage entre des abonnés.

- **Liste grise (*greylists*)** : technique de filtrage basée sur le blocage temporaire des courriers électroniques reçus, conduisant le destinataire à devoir confirmer sa légitimité.

- **Liste noire (*blacklists*)** : liste répertoriant les adresses électroniques, noms de domaines ou adresses Ip d'expéditeurs connus comme « spammeurs » et permettant ainsi de reconnaître et de bloquer tout courrier électronique en provenance de ces adresses ou domaines.

- **Logiciel malveillant (maliciel) (*malware*)** : programme introduit dans un système informatique à l'insu de son propriétaire et constituant une menace pour son système (endommagement du système ou détournement de la finalité initialement prévue par son propriétaire (entrent dans cette catégorie : virus, cheval de Troie, portes dérobées, vers, etc.).

- M -

- ***Mail bombing:*** attaque consister à envoyer massivement des *e-mails* dans le seul but de nuire à la victime (saturation de sa messagerie électronique, par exemple).

- ***Mail Harvesting*** : technique qui consiste à parcourir un grand nombre de ressources publiques (pages *Web*, groupes de discussion, sites de réseaux sociaux, etc.), afin d'y collecter les adresses électroniques à des fins malveillantes.

- ***Mailing list*** **(v.** Liste de diffusion)

- **MDA (*Mail Delivery Agent*)** : serveur de courrier électronique qui délivre les messages entrants et les stocke dans le système de fichiers.

- **Messagerie électronique :** Service de transmission de courriers électroniques.

- **Messagerie instantanée (*Instant Messaging,* IM) :** messagerie synchrone qui offre la possibilité de recevoir et d'envoyer des messages de façon instantanée.

- ***Messenger spam (spam-up)*** **:** *spam* qui se répand sur les messageries instantanées.

- **Moteur de recherches :** application destinée à trouver des ressources sur le *Web* à partir d'une requête composée de mots-clés choisis par l'internaute.

- **MUA (*Mail User Agent*)** : logiciel installé sur les postes de travail qui sert à rédiger, envoyer et consulter les messages reçus (par exemple, *Mozilla Thunderbird, Microsoft Outlook, Lotus Notes…*).

- **MTA (*Mail Transfert Agent*) :** serveur de messagerie électronique chargé de l'acheminement des *e-mails* d'un serveur vers un autre serveur.

- N -

- **Noms de domaine** : Suite de caractères associée à une adresse IP de la forme www. , nom d'une entreprise, d'une association, d'une marque et suivie d'une extension (.fr, .com…).

- O -

- ***Open relay*** : (v. *Relais ouvert)*

- P -

- **PC zombie (*bot*) :** ordinateur infecté par un logiciel malveillant qui est contrôlé à distance pour mener des attaques contre d'autres systèmes informatiques.

- ***Phishing :*** contraction des termes « *fishing* » (pêche) et « *phreaking* » (fraude informatique). Il s'agit d'une fraude informatique qui consiste à usurper l'identité d'un prestataire connu (un établissement bancaire, une autorité publique, un portail …) afin de soutirer des informations confidentielles (identifiant, mot de passe et autres données à caractère personnel).

- **Pixel invisible (*Web bug*)** : minuscule graphique implanté dans une page *Web* ou un courrier électronique et destiné à surveiller la consultation de cette page ou de ce message, à l'insu des lecteurs afin d'alerter le « spammeur » dès que le message est lu.

- **POP3 ou IMAP** : protocoles permettant de relever les messages pour leur lecture.

- **Pop-up:** fenêtre publicitaire qui s'ouvre automatiquement lors d'une connexion à l'internet.

- **Pot de miel** : ordinateur ou programme créé pour attirer et piéger les pirates informatiques.

- ***Proxy***: (ou « serveur mandataire ») serveur informatique dont le rôle est de servir de relai entre un client (un particulier, une entreprise) et un serveur (le site internet consulté).

- **Publipostage** : technique *marketing* consistant à envoyer en nombre des informations ou des prospectus publicitaires, par voie postale ou électronique, destinée à promouvoir un produit ou un service.

- R -

- **Rapport de non remise (NDR)** : type de notification généré chaque fois qu'un message ne peut être transmis à son destinataire. Si un serveur détecte la cause de cet échec de remise, il l'associe alors à un code d'état et un message d'erreur correspondant est rédigé.

- ***Registrant :*** personne qui a enregistré un nom de domaine.

- ***Relais ouvert :*** serveur de messagerie non protégé ou mal protégé autorisant tout envoi de messages sans authentification préalable de l'expéditeur. Leur utilisation permet ainsi de masquer l'origine des messages.

- ***Remailer*** **anonyme** : serveur qui assure l'expédition des courriers électroniques de façon anonyme en supprimant toutes les informations permettant d'identifier l'expéditeur à l'origine de l'envoi.

- **Réseaux de PC zombies (*botnet*)** : ensemble d'ordinateurs compromis (zombies).

- **Réseau social :** site Internet qui permet de regrouper une communauté d'internaute, reliés entre eux par des centres d'intérêts communs, une profession commune ou similaire et facilitant leurs échanges d'informations, d'images, de fichiers musicaux…

- **Robot d'indexation (*Web crawler* ou *Web spider*)** : logiciel permettant de parcourir le *Web* à la recherche du signe @ et collecter ainsi les adresses électroniques.

- **ROSKO (*Register of Known Spam Operations*)** : liste élaborée par le *Spamhaus Project* répertoriant les « spammeurs » identifiés comme les plus menaçants et qui ont été chassés plus de trois fois par leur FAI.

- S -

- ***Scam*** (v. escroquerie à la nigériane)

- ***Sender Policy Framework*** **(SPF) :** extension du protocole SMTP qui vérifie la légitimité d'un *e-mail* en comparant le domaine de l'*e-mail* de l'expéditeur avec une liste d'ordinateurs autorisés à envoyer des courriers électroniques à partir de ce même domaine.

- ***Sender*** **ID:** norme d'authentification du nom de domaine de l'expéditeur d'un courrier électronique.

- **Serveur de messagerie :** ordinateur dans un réseau (ou logiciel exécutant ce service) stockant les *e-mails* entrants pour leur distribution aux utilisateurs et acheminant les *e-mails* sortants.

- **SMS (*Short Message Service*)** : message textuel limité en général à 160 caractères transmis d'un téléphone mobile à un autre.

- **SMTP** : protocole de communication qui établit la connexion entre le serveur d'un expéditeur et celui d'un destinataire afin de permettre l'envoi de courrier électronique. Destiné à acheminer les messages, le protocole SMTP fonctionne conjointement avec les serveurs POP (*Post Office Protocol*) qui permet de récupérer l'*e-mail*.

- S***pamware*** **:** logiciel dédié à l'envoi massif de *spams*.

- ***Spambot*** *:* robot d'indexation malveillant utilisé par les « spammeurs » pour collecter sur le *Web* les adresses électroniques.

- ***Spamdexing*** **:** ensemble de techniques de référencement abusif consistant à tromper les moteurs de recherche sur la qualité d'une page ou d'un site *Web* et obtenir de manière artificielle un bon référencement dans les résultats des moteurs de recherche.

- ***Spamhaus Block List*** **(SBL) :** liste élaborée par le *Spamhaus Project* regroupant les adresses IP de « spammeurs » connus.

- ***Spam*** **SMS** : *spam* envoyé sur les mobiles sous la forme de *Sms*.

- **SPIM (*Spam Over Instant Messaging*)** : *spam* qui est envoyé par le biais d'un programme de messagerie instantanée.

- **SPIT** : (acronyme de *Spam over Internet Telephony*) publicité indésirable réalisée *via* les réseaux de communication téléphonique sur IP.

- ***Spoofing*** : technique consistant à usurper l'identité d'un internaute, notamment en falsifiant son adresse électronique ou son adresse IP, afin de laisser croire que des courriers électroniques expédiés proviennent de cet internaute.

- T -

- **Téléphonie sur IP :** technique qui permet de communiquer oralement *via* l'internet ou *via* tout autre réseau qui accepte le protocole TCP/IP.

- **Terminal:** équipement situé en extrémité d'un réseau de télécommunication, communiquant sur ce réseau et qui assure en général l'interface avec l'utilisateur.

- **Test de *Turing :*** technique de filtrage consistant à renvoyer un courrier électronique de demande d'authentification (en reproduisant un code affiché) à l'expéditeur d'un message destinée à s'assurer de son existence physique réelle.

- ***Trojan*** (v. cheval de troie)

- U -

- ***Usenet*** : acronyme de « *Users' network* », réseau d'ordinateurs qui transfert des articles publiés sur des forums de discussion, permettant l'échange de contributions sur un thème donné entre les membres d'une communauté.

- V -

- **Virus :** Par analogie avec le terme biologique, il s'agit d'un code caché qui se propage par contamination d'un programme qui peut un dysfonctionnement de l'ordinateur infecté.

- W -

- ***Whitelist*** (v. liste blanche)

- **WIFI :** technologie d'accès sans fil permettant la connexion à l'internet dans un rayon limité à quelques dizaine de mètres (enivrions 80 - 100 mètres).

- Z -

- **Zombie :** ordinateur infecté par un virus et contrôlé à distance par un « spammeur » à des fins d'envois de *spams*.

INDEX

- Les chiffres correspondent aux numéros des paragraphes, les chiffres en gras indiquent les passages les plus importants.
- Les chiffres en italique indiquent que le mot indexé se trouve en note de bas de page.

- A -

Abus de qualité vraie 395

Accès (à un système) 369, 371 à 375

Accès (droit d') 227à 229

Action de groupe 491 et s.
- certification 500
- v. dommage de masse 502
- jugement 503
- mandat 501

Action frauduleuse (sur les données) 425 à 429

Adresse IP 66, 89, 116, 132, 139, **187**

Adresse Mac 167, 187

Adresse électronique
- captation et utilisation abusive 83 et s.
- donnée à caractère personnel 37, **184 à 186**
- enjeu commercial 147 à 149
- procédés de collecte 91 à 93
- vérification de la validité 94

Adresse professionnelle 319

Agence Européenne chargée de la sécurité des réseaux et de l'information 526

American Standard Code for Information Interchange 123

Annuaire (d'adresses) 17, 59, **86**, 93

Anonymat 95, 138, 139, **165**
- discours anonyme (v. *Jeremy Janes v. Commonwealt of Virginia)*
- v. *mail bombing*

Anti-*spam* (loi)
- v. *CAN-SPAM Act*
- v. LCEN

Appairage 249

ARCII Art (v. *American Standard Code for Information Interchange*)

Arnaque 104, 105

Arnaque à la nigériane 107, 398, 400, 555

Article 14 et 15 du Code civil
- caractère subsidiaire 543, 554, **556**
- nationalité française 557

Article 3 alinéa 1er du Code civil 579

Article 5.3 du règlement Bruxelles I 544

Articles 42 et 46 du Code de procédure civile 544, 555

Asia-Europe Meeting 526

Attaque dictionnaire 93, 122

Attribut de la personnalité
- v. patrimonialisation

Authentification
- v. cryptage
- v. *Domain Keys Identified Mail*
- v. Sender ID
- v. SPF

- B -

Balancing approach 153

Bande passante 49, 56, 96, 159, 381, 452, 461, 463

Bayesien (filtrage) 124 à 126

Blacklist (v. liste noire)

Blog 59, **99**, 176, 236

Blue spam 100, 192, 298, 311, 322, 356

Bluetooth 167, 183, **187**, **192**, **197**
- v. adresse MAC
- v. *Blue spam*
- donnée à caractère personnel 187
- v. identifiant *Bluetooth*

Bot (v. PC zombie)

Botnet **(**v. réseau de zombies)

- C -

CAN-SPAM Act 323 et s.
- régime des envois commerciaux 328 à 334
- responsabilité 336 à 345
- sanctions 346 à 352

Case à cocher 224, 306, **309**

Causalité adéquate 460

Central Hudson 156 et s.
- v. *Jeremy Janes* v. *Commonwealt of Virginia*

Certain (caractère du dommage) 453 à 455

Chaîne de courriers électroniques

Children's Online Privacy Protection Act 264

Class action 496 et s.
- application au dommage de masse 498
- déroulement 497
- exemple de la class action américaine 496

Clause d'exception 569, **574 à 576**

CNIL (Commission Nationale Informatique et Libertés) 247 à 249, 257 à 259

CNSA (*Contact Network of Spam Authorities*) 526

Code de bonne conduite 507

Collecte
- v. information (obligation d')
- principe directeurs en matière de collecte et de traitements des données 195 à 209
- procédés 91 à 93

Commerce personnalisé 147
- v. *data mining*
- v. *profiling*
- v. segmentation comportementale
- v. *scoring*

CompuServe, Inc. v. Cyber Promotions 442, 443
- dommage 456 à 459
- faute 448
- *trespass to chattels* 442 et s.

Confidentialité (obligation de) (v. sécurité)

Conflit de juridictions (v. règlement Bruxelles I)

Conflit de lois (v. règlement Rome II)

Consentement préalable 196, 197, 257, 285, 286, 295 et s.

Contestation (droit de) 231

Convention de Rome sur la loi applicable aux obligations contractuelles 564

Cookie 166, 220, 371

COPPA (v. *Children's Online Privacy Protection Act*)

Cost-shifting 8

Courrier électronique
- contenu 22, 105, 106,
- définition 19, **297**, **298**
- envoi/réception massive 13, 44, 49, 50, 52, 56, 77, 109
- faux 29
- v. filtre anti-*spam*
- v. *mail bombing*
- non sollicité **14**, 60
- perte 48, 55, 60
- v. *phishing*
- v. pratique commerciale trompeuse
- support du *spamming* 19

Critère de rattachement
- conflit de juridictions 543 à 545, 556, 558
- conflit de lois
  - atteinte aux droits de la personnalité 579, 582
  - matière délictuelle 570 et s., 574 et s.

Customer Relationship Management
- v. gestion de la relation client

Cryptographie 132, 134, 135, 213

CyberPromotions, Inc. v. America Online
- constitutionnalité des techniques de filtrage 155
- liberté d'expression commerciale 155

Cybertrespass 439
- v. *trespass to chattels*

- D -

Data mining 148

***Data Privacy Act and Security of* 2009** 271 à 279

Déclaration (des traitements de données) 211, 212

Délit complexe
- définition 518, 519
- règlement Bruxelles I 546
- règlement Rome II 577, 580, 581

DHA (attaque dictionnaire)

Directive
- directive 2000/31/ CE du Parlement européen et du Conseil du 8 juin 2000 relative a certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur 291
- directive 2002/58/ CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données a caractère personnel et la protection de la vie privée dans le secteur des communications électroniques 19, 33, 214, **293**
- directive n° 2005/29/Ce du 11 mai 2005 relative aux pratiques commerciales déloyales des entreprises vis-à-vis des consommateurs dans le marché intérieur 406, 408, 410
- directive 2009/136/ CE du Parlement européen et du Conseil du 25 novembre 2009 modifiant notamment la directive 2002/58/ CE concernant le traitement des données a caractère personnel et la protection de la vie privée dans le secteur des communications électroniques 214, 298, 321
- directive 95/46/ CE du Parlement européen et du Conseil du 24 octobre 1995 relative a la protection des personnes physiques à l'égard du traitement des données à caractère personnel et a la libre circulation de ces données 135, 180, 201, 233, 262, 293
- directive 97/66/ CE du Parlement européen et du Conseil du 15 décembre 1997 concernant le traitement des données a caractère personnel et la protection de la vie privée dans le secteur des télécommunications 291, 292
- directive 97/7/ CE du Parlement européen et du conseil du 20 mai 1997 concernant la protection des consommateurs en matière de contrats a distance 291, 292

Directory Harvest Attack (v. attaque dictionnaire)

Discours commercial (v. liberté d'expression commerciale)

DKIM (v. *Domain Keys Identified Mail*)

DNS 132 A 135

Domaine (nom de) 5, 115, 117, 122, 132 à 137, 142

Domain Keys Identified Mail
- v. cryptographie

Domicile 515, 522, 541, 542, **543**, **548**, 550, **554**, **558**, **559**, 560, 561, 572 à 575, **582**

Dommage 44 et s., 450 et s.
- appréciation par les cours américaines 456 à 459
- caractères 453 à 455
- économique 451
- matériel 451
- moral 451
- v. réparation
- *spamming* 44 à 50, 452, 455

Dommage de masse 493, 494, 495 et s.
- action de groupe en droit français 499 et s.
- v. *class action*

Dommages-intérêts punitifs 478 à 490

Donnée à caractère personnel
- v. adresse électronique
- v. collecte
- définition 184 à 186
- donnée *Bluetooth* 187
- v. informatique, fichiers et libertés
- v. patrimonialisation
- v. traitement

Donnée nominative (v. donnée à caractère personnel)

Droit (des titulaires de données)
- à l'oubli numérique (v. oubli)
- d'accès (v. accès)
- de contestation (v. contestation)
- de rectification (v. rectification)
- d'opposition (v. opposition)

Droit à être laissé tranquille 171, 173

Droit à la protection des données 169 et s.
- droit de la personnalité 170
- droit de propriété 169
  - exploitation commerciale de l'usage de données 171

Droit comparé 70 à 74

Droit de la personnalité 170
- loi applicable (v. art. 3 al. 1er C. civ.) 578 et s.

Droit international privé
- v. délit complexe
- v. règlement Bruxelles I
- v. règlement Rome II
- *spamming*
  - délit plurilocalisé 518, 519
  - spécificités 520, 522

Droit patrimonial 171

Droit pénal de la consommation 404 et s.
- v. pratique commerciale
- v. pratique commerciale agressive
- v. pratique commerciale trompeuse

Droit pénal de l'informatique 367 et s.
- v. action frauduleuse
- v. intrusion
- v. perturbation
- v. système

- E -

E-mail (v. courrier électronique)

ENISA (*European Network and Information Security Agency*)
- v. Agence Européenne chargée de la sécurité des réseaux et de l'information

Entrave (au fonctionnement du système) 376 à 381

Équivalence des conditions 460

Escroquerie 384 à 403
- condition préalable 386 à 389
- élément matériel 390à 401
- élément moral 402
- sanctions 403

Escroquerie a la charité 397

Escroquerie a la nigériane (v. arnaque à la nigériane)

Escroquerie a la publicité 397

Espaces publics de l'internet 16, **83**

Extranéité 528, 531, 567, 587

- F -

FAI
- dommage 46 à 51, 56
- LCEN 321
- v. *trespass to chattels*

Fausse qualité 392, 394, 398, 400

Fausser (le système) 378 à 380

Faute 446 et s.
- appréciation par les cours américaines 448
- intention 449

Faute lucrative 472 à 477
- sanction (v. dommages-intérêts punitifs)

Faux négatif 117, 121, 123, 126

Faux nom (escroquerie) 392, 393, 398, 400, 402

Faux positif 50, 116 à 118, 121, 128

Filtre anti-*spam*
- constitutionnalité (*CyberPromotions, Inc. v. America Online*) 155
- en fonction de l'origine des messages 113 à 118
  - v. liste blanche
  - v. liste grise
  - v. liste noire
- en fonction du contenu des messages119 à 126
  - v. bayesien
  - v. heuristique
  - par mots-clés
- *Turing* 127 à 129

Finalité (principe de) 201 à 203

***Fiona Shevill* 547**, 551

Forum de discussion 11, 17, 59, 83, **84**, **99**, 165, 203, 218, 221, 236, 507

Forum non conveniens 545

Forum shopping 564, 583

Fournisseur de messagerie (v. FAI)

FTC 141, 264, 331, 332, 336, 338, 339, 343, 346, 347

- G -

G29 (Groupe de l'article 29) 135, 309, 317, 318

Gestion de la relation client 147

Greylists
- v. liste grise

- H -

Harvesting
- v. robot " aspirateur "

Hashbusting 120

Heuristique (filtrage à) 122, 123

Hoax 87

HoneyPot **(**v. pot de miel)

- I -

Identifiant *Bluetooth* 187, 197

Information (obligation d') 216 à 221

Informatique, fichiers et libertés (loi IFL)
- principe directeurs en matière de collecte et de traitements des données 195 à 209
- obligation en matière de collecte et de traitement 210 à 221
- droits des titulaires de données 223 à 238
- volet pénal 239 à 259

Information nominative (v. donnée à caractère personnel)

Ingénierie sociale *54*

IP (adresse) 63, 89, 116, 118, 130, 132, 139
- donnée à caractère personnel 187

Installations essentielles (doctrine des) 150

Instance internationale 525 et s.

Intrusion (dans un système) 368 à 375

- J -

Jeremy Janes v. Commonwealt of Virginia (droit au discours anonyme) 161

- K -

Keywords stuffing 34

- L -

LAP
v. *London Action Plan*

Labellisation 329

Lautour 579, 580

LCEN (Loi pour la confiance dans l'économie numérique) 294 et s.
- champ d'application 296 à 302
  - v. courrier électronique
  - destinataires 299
  - v. prospection directe
- exceptions
  - v. adresse professionnelle
  - relations commerciales préexistantes 315 à 318
- sanctions
- transparence des envois 304 à 311
  - consentement préalable (*opt-in*) 305 à 311
  - droit d'opposition 312-313

Légitimité (principe de) 196, 197

Lettre d'information 13, 83

Lex loci damni 570 à 572

Lex loci delicti 570, 574

Liberté d'expression (v. Premier Amendement)

Liberté d'expression commerciale 150 et s.
- v. *balancing approach*
- v. *Central Hudson*
- v. *CyberPromotions, Inc. v. America Online*
- v. *Jeremy James* v. *Commonwealth of Virginia*
- v. *Rowan v. United States Post Office Dept.*

Lien de causalité 460 et s.
- v. causalité adéquate
- v. équivalence des conditions

Liste banche 117

Liste de diffusion 59, 83, 85, 203, 221

Liste grise 118

Liste noire 114 à 116

Logiciel aspirateur 59, 200, 218, 330, 332, 349, 357

Logiciel malveillant 84, 97, 104, 381, 429

Loi
- loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique 294 et s.
- loi n° 2004-669 du 9 juillet 2004 relative aux communications électroniques et aux services de communication audiovisuelle *838*
- loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques a l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative a l'informatique, aux fichiers et aux libertés (v. informatique, fichiers et libertés)
- loi n° 2007-1544 du 29 octobre 2007 de lutte contre la contrefaçon 475
- loi n° 2008-3 du 3 janvier 2008 pour le développement de la concurrence au service des consommateurs, dite " loi Chatel " 405 et s.
- loi n° 2008-776 du 4 août 2008 de modernisation de l'économie, dite " loi LME " 405 et s.
- loi n° 73-1193 du 27 décembre 1973, d'orientation, du commerce et de l'artisanat, dite " loi Royer " 421
- loi n° 78-17 du 6 janvier 1978 relative à l'Informatique, aux fichiers et aux Libertés (v. informatique, fichiers et libertés)

London Action Plan 527
- v. *Operation Secure Your Server*
- v. *Operation Zombies*

Loyauté (principe de) 198 à 200
- aspiration des adresses 200

LTU c/ Eurocontrol *1642*

- M -

Marinari 559

Mail bombing 13, **30**, 38, 55, 56, 60, **96**, 172, **375**, **381**, 382, 431, **452, 455**

Mail harvesting (v. robot « aspirateur »)

Mailing list (v. liste de diffusion)

Maintien (dans un système) 370 à 375

Maliciel (v. logiciel malveillant)

Malware (v. logiciel malveillant)

Manœuvres frauduleuses 396, 397, 400, 402

Marketing one-to-one
- v. commerce personnalisé

Mensonge 391, 396, 397

Messagerie électronique 7, 13, 22, 30, 33, 52, 60, 109, 110, 137, 160, 172, 263, 508, 511, 550

Messagerie instantanée(v. *spim*)

Messenger spam (v. *spam-up*)

***Mines de Potasse* 546**, 547, 548, 551

Moteur de recherches 11, 34, 166, 236, 237

MTA 137

- N -

Nationalité française (v. art. 14 et 15 du C. civ.)

NDR (v. rapport de non-remise)

Neutralité (de la règle de conflit) 534, 564, 576

Newsgroup (v. forum de discussion)

Newsletter (v. lettre d'information)

Nom patronymique
- v. droit de la personnalité
- v. droit patrimonial
- v. patrimonialisation

- O -

OCDE 321, 525, 526

Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication *216*

Open relay (v. relais ouvert)

Operation Secure Your Server 527

Operation Zombies 527

Opposition (droit d')
- *CAN-SPAM Act* 331, 332
- LCEN 312, 313
- loi informatique, fichiers et libertés 224 à 226

Opt-in 285, 286, **294 et s.**

Opt-out 287, 288, **327 et s.**

Oubli (droit a l') 233 à 237
- anonymat 235

- P -

Patrimonialisation 171

PC zombie 60, 97, 104, 116, 138, 366, 375, 381, 431,**452**, **455**, 527, **555**, **573**, **581**
- v. *botnet*
- v. administrateur de zombies

Pelassa *1673*
Perte de chance
- dommage 454, 455
- évaluation 465

Pertinence (principe de) 205, 206, 209

Perturbation (du fonctionnement du système) 376 à 381

Phishing
- v. arnaque à la nigériane

Ping-call (v. *spam* par téléphone)

Pixel invisible 94

Plateforme d'alerte 33 700 89, *242*

POP3 ou **IMAP** 137

Pop-up 33

Pot de miel 130, 131

Pratique commerciale 406 à 412

Pratique commerciale agressive 421

Pratique commerciale trompeuse 413 à 423

Premier Amendement 151, 152, 154 à 156, 158, 161, 324

***Privacy Act of* 2005** 267 à 270

Profiling 148

Projet CATALA 447, 464, 471, 477, 483, 485 à 488

Proportionnalité 207 à 209

Proposition de loi portant réforme de la responsabilité civile 453, 464, 465, 477, 483, 485, 487, 488

Prospection directe 300 à 302

Protocole IPv6 95

Proximité (v. clause d'exception)

Proxy 89, 581

Publipostage 4, 7, 13, 173, 216 à 218, 282, 285, 292, 358, 404, 439

- Q -

Qualification (droit international privé) 535 à 537

- R -

Rapport de non-remise 94

Rectification (droit de) 198, 216, 218, 220, **230 à 232**

Registrant 352

Registre (d'*opt-out*) 332

Règlement
- règlement (CE) n° 44/2001 du Conseil du 22 décembre 2000 concernant la compétence judiciaire, la reconnaissance et l'exécution des décisions en matière civile et commerciale (v. règlement Bruxelles I)
- règlement (CE) n° 864/2007 du Parlement européen et du Conseil sur la loi applicable aux obligations non contractuelles du 11 juillet 2007 (v. règlement Rome II)

Règlement Bruxelles I 538 et s.
- v. *Fiona Shevill*
- v. *Mines de Potasse*
- v. article 5.3 du règlement Bruxelles I
- v. articles 14 et 15 du Code civil

Règlement Rome II 532 et s.
- loi application aux atteintes aux droits de la personnalité 579 et s.
- loi applicable aux délits 563 et s.
    - v. ég. clause d'exception

Relais ouvert 95, **140**, 330

Remailer 89, 95, 139

Réparation 462 et s.
- intégrale 463 et s.
    - limites 467 à 469
    - modalités 464
    - négligence de la victime 466
    - perte de chance 465

Réseau de zombies (v. PC zombie)

Réseaux sociaux 22, **88**, **102**, 176, 218, 221, 236, 265

Résidence habituelle (v. domicile)

Résiliation 508

Responsabilité civile délictuelle 433 et s.

Responsabilité contractuelle 505 et s.

Responsabilité pénale 365 et s.

Responsable de traitement 193
- v. traitement

Restatement 448, *317, 1248, 1250, 1253, 1255, 1256, 1261-1263*

Robot d'indexation 92

ROSKO (*Register of Known Spam Operations*) 6

***Rowan** v. United States Post Office Dept.* 153

- S -

Safer Internet Plus 526

Scam
- v. escroquerie a la nigériane

***Scheffel** 1673*

Scoring 148

Sécurité (obligation de) loi IFL : 213 à 215
- définition
- obligation renforcée
- *spamming*

Segmentation comportementale *310*

***Sender* ID** 132, 133

Service public 150

SMS 6, 19, 89, 101, 183, 291, 292, 295, 297, 312

SMTP 97, 132, 136, 137

SPF (v. *Sender Policy Framework*)

SPIT
- v. téléphonie sur IP
- v. voix sur IP (VOIP)

Spambot 92

Spamdexing 34

Spamhaus Block List

« Spammeur »
- association aux auteurs de virus 104
- profil
- v. responsable de traitement
- v. *spamming*

Spamming
- v. adresse électronique
- v. *CAN-SPAM Act*
- cibles d'envoi 99 à 102
- contenus plus dangereux 27 à 31
- coût 46 à 51
- définition 11 à 24
- v. délit complexe
- v. droit international privé
- histoire 2 à 5
- impact général 45 à 53
- impact individuel 54 à 60
- v. informatique, fichiers et libertés
- v. LCEN
- v. liberté d'expression commerciale
- mutations 98 à 107
- origine du terme 1
- raison de l'essor 8
- v. responsabilité civile contractuelle
- v. responsabilité civile délictuelle
- v. responsabilité pénale
- technique de prospection unique 7
- techniques d'envoi 95 à 97
- techniques exclues 32 à 34
- v. *trespass to chattels* 435 et s.

- vecteur d'escroqueries
  - v. escroquerie

Spam-up 33

***Spam* vocal** 297, *242*
- v. office central de lutte contre la criminalité liée aux technologies de l'information et de la communication

Spamware (v. *harvesting*)

SPIM 100

Spoofing (usurpation du nom de domaine)

Sté Dumez c/ Hessische Landesbank *1661*

Système (de traitement automatise de données)
- définition 367
- v. droit pénal de l'informatique

- T -

Téléphonie sur IP 101

Terminal 33, 167, 187, 297, 311

***Thrifty-Tel, Inc. v. Bezenek* 440**, 441, 442, 448

Toolkit Anti-spam 525

Traitement (de données) 188 à 192
- Loi IFL
  - principe 195 à 209
  - obligation des responsables de traitement 210 à 221
- *Personal Data Privacy Act and Security of 2009* 272 à 275

Transparence (des envois)
- v. *CAN-SPAM Act* 328 à 330
- v. LCEN 304 à 311

Trespass to chattels 435 et s.
- conditions 435 à 438
- v. *CyberPromotions, Inc. v. America Online*
- v. *Thrifty-Tel, Inc. v. Bezenek*

Tromperie
- v. abus de qualité vraie
- acte positif
- v. escroquerie à la charité
- v. escroquerie a la publicité
- v. fausse qualité
- v. faux nom)
- insuffisance du simple mensonge (v. mensonge)
- v. manœuvres frauduleuses)
- v. tromperie par action
- v. tromperie par omission

Tromperie par action 415 à 419

Tromperie par omission 420

Turing (test de) 127 à 129

- U -

UIT (Union Internationale des Télécommunications) 526

Usenet 3, 4, 22, 99, 100

Usurpation du nom de domaine 137

- V -

Virus 27 à 29, 31, 38, 84, 87, **97**, **104**, **378**, **379**, **381**, **426**, **429**, 460
- v. logiciel malveillant

Voix sur IP (protocole)
- v. téléphonie sur IP

- W -

Web bug
- v. pixel invisible

Web crawler (v. robot d'indexation)

Web spider (v. robot d'indexation)

Whitelist (v. liste blanche)

WIFI 138, 167

- Z -

Zombie (v. PC zombie)

PLAN DÉTAILLÉ

REMERCIEMENTS **7**

RÉSUMÉ et MOTS-CLÉS **9**

PRINCIPALES ABRÉVIATIONS **11**

NOTE À L'ATTENTION DES LECTEURS **18**

PLAN SOMMAIRE **21**

INTRODUCTION GÉNÉRALE **23**

§ 1. L'OBJET DE LA RECHERCHE 30

A. Le *spamming* 30

1. Analyse des critères de définition retenus par la CNIL 32

2. La recherche d'autres critères de définition objectifs 35

3. La nécessaire prise en compte des diverses formes de *spamming* : l'accroissement des dangers 37

a. Des contenus plus dangereux 37

b. Des méthodes d'envoi de plus agressives 39

4. Techniques exclues 39

B. Le *spamming,* au carrefour d'une pluralité de droits 40

1. La diversité des droits sollicités 41

2. Les questions de droit international 43

§ 2. LES INTÉRÊTS DE LA RECHERCHE 45

A. L'intérêt pratique : Un besoin de protection des « spammés » 45

1. L'impact général 46

a. L'impact sur les entreprises et les FAI 46

b. L'impact sur la communauté des internautes 48

2. L'impact individuel 49

a. L'impact sur un « spammé », entreprise ou FAI 50

b. L'impact sur un « spammé », internaute 51

i. La menace sur les données à caractère personnel 51

ii. L'atteinte subie par la réception d'un spam 53

B. L'intérêt théorique : Le droit face aux nouvelles technologies 55

§ 3. LA MÉTHODE DE LA RECHERCHE 60

A. La démarche générale 61

B. La démarche de droit comparé 66

PREMIÈRE PARTIE LES IMPERFECTIONS DE LA PROTECTION SPÉCIALE **71**

TITRE PREMIER : LA MULTIPLICITÉ DES DÉFIS FACTUELS **74**

CHAPITRE PREMIER : LE DÉFI TECHNOLOGIQUE **75**

SECTION I. UN ENVIRONNEMENT TECHNOLOGIQUE HOSTILE 76
§ 1. DES DONNÉES FORTEMENT EXPOSÉES À DES CAPTATIONS ET UTILISATIONS ABUSIVES 76
§ 2. LES RÉALITÉS PRATIQUES DE LA MENACE : LE *MODUS OPERANDI* DES « SPAMMEURS » 80
A. Les techniques de collecte des adresses électroniques 80
B. Les techniques de vérification de la validité des adresses 82
C. Des techniques d'envois de plus en plus pernicieuses et agressives 83
D. Les mutations du *spamming* 85
1. Des cibles d'envoi multiples 85
2. Du *spamming* commercial au *spamming* malveillant 88
a. La connivence entre « spammeur » et auteur de virus 88
b. Le *spamming*, vecteur d'escroqueries 89
SECTION II. L'ÉCHEC D'UNE RÉPONSE EXCLUSIVEMENT TECHNIQUE 93
§ 1. L'INSUFFISANCE DES DISPOSITIFS TECHNIQUES DE PROTECTION 93
A. Les techniques de filtrage, un outil aléatoire 94
1. L'inefficacité des filtrages programmés en fonction de l'origine des messages 95
a. Les listes noires, une technique aux multiples failles 95
b. Les listes banches, facteur de blocage des flux d'*e-mails* 96
c. Les listes grises, frein à une communication rapide des *e-mails* 97
2. L'inefficacité des filtrages programmés en fonction du contenu des messages 97
a. Le filtrage par mots-clés, un procédé élémentaire inopérant 97
b. Le filtrage à heuristique, un procédé plus élaboré mais toujours fragile 98
c. Le filtrage Bayesien, un procédé d'analyse subtil mais d'effectivité limitée 99
3. Le test de *Turing*, un risque important de faux positifs 101
B. Les *HoneyPots*, une technique surannée 102
C. Les techniques basées sur l'authentification, un palliatif prometteur 102
§ 2. LES NOUVELLES TECHNOLOGIES DE COMMUNICATION AU SERVICE DES « SPAMMEURS » 105
A. Les difficultés techniques de suivi du parcours des *spams* 105
B. Les difficultés techniques de traçage des flux financiers 107
Conclusion du Chapitre 1 109

CHAPITRE SECOND : LES DÉFIS SOCIO-ÉCONOMIQUES 110

SECTION I : LES MOTIVATIONS ÉCONOMIQUES ET JUSTIFICATION AU SOUTIEN DU *SPAMMING* 111
§ 1. LES ADRESSES ÉLECTRONIQUES, UNE SOURCE POTENTIELLE DE PROFITS 111
§ 2. LE *SPAMMING* JUSTIFIÉ AU NOM DE LA LIBERTÉ D'EXPRESSION COMMERCIALE 115
A. Une protection relative du discours commercial 117
B. La liberté d'expression à l'épreuve du *spamming* 120
1. La question de la constitutionnalité des techniques de filtrage 120
2. La question de la constitutionnalité des lois anti-*spam* 121
SECTION II. UNE INQUIÉTUDE SOCIALE CROISSANTE 127
§ 1. LA PERTE DE CONTRÔLE DES TITULAIRES SUR LEURS DONNÉES 127
A. Une identité numérique aisément accessible, source de dérives 127
B. La revendication d'un droit à la protection des données 131

§ 2. LA REVENDICATION D'UN DROIT À ÊTRE LAISSÉ TRANQUILLE 138
Conclusion du Chapitre 2 142
Conclusion du Titre 1 143

TITRE SECOND : DES LÉGISLATIONS SPÉCIALES FRAGILES 145

CHAPITRE PREMIER : DES LOIS DE PROTECTION DES DONNÉES INCOMPLÈTES FACE AUX MENACES DU *SPAMMING* 146

SECTION I. EN FRANCE, UNE PROTECTION UNIFORME À RENFORCER 147
§ 1. LE *SPAMMING,* UNE PRATIQUE SOUMISE AU RESPECT DE LA LOI INFORMATIQUE, FICHIERS ET LIBERTÉS 148
A. La collecte de données à caractère personnel par le « spammeur » 149
1. L'adresse électronique, une donnée à caractère personnel 149
2. La question de la nature juridique des données *Bluetooth* 152
B. Les traitements de données opérés par les « spammeurs » 155
§ 2. LE *SPAMMING*, UNE PRATIQUE EN VIOLATION DE LA LOI INFORMATIQUE, FICHIERS ET LIBERTÉS 158
A. Des obligations légales transgressées par les « spammeurs » 158
1. Le non-respect des principes directeurs gouvernant la collecte et les traitements de données 159
a. Le principe de légitimité 159
b. Le principe de loyauté 160
c. Le principe de finalité 163
d. Les principes de pertinence et de proportionnalité, corollaires du principe de finalité 164
i. Le principe de pertinence 165
ii. Le principe de proportionnalité, prolongement du principe de pertinence .. 166
iii. Une mise en œuvre délicate de ces deux principes 167
2. Le non-respect des obligations en matière de collecte et de traitement 168
a. L'obligation de déclaration des fichiers d'adresses électroniques 168
b. Les obligations de sécurité et de confidentialité des données 171
c. L'obligation d'information 174
B. Des droits ignorés par les « spammeurs » 178
1. Le non-respect du droit d'opposition, prolongement du devoir d'information 178
2. La reconnaissance d'un droit d'accès 180
3. Le droit de rectification, corollaire du droit d'accès 182
4. Le droit à l'oubli numérique, une prérogative ignorée par le droit ? 183
§ 3. LE VOLET RÉPRESSIF : UN BILAN DÉCEVANT 191
A. Un arsenal pénal prometteur en théorie 192
1. Une sévérité accrue dans les textes 192
a. La multiplication des textes d'incrimination 192
b. L'aggravation des sanctions fixées 194
2. Le renforcement des pouvoirs de la CNIL 196

B. Une mise en œuvre décevante en pratique 199
1. Les imperfections rédactionnelles de la loi pénale, source d'insécurité juridique .. 199
2. Un contentieux rare et faiblement sanctionné 201
3. La CNIL, une main-forte insuffisante à la loi pénale 203
SECTION II. AUX ÉTATS-UNIS, UNE PROTECTION CONTRASTÉE À UNIFORMISER 207
§ 1. AVANT 2005 : UN PANORAMA LÉGISLATIF DÉSORDONNÉ 208
§ 2. À PARTIR DE 2005 : LES PRÉLUDES Á UNE PROTECTION PLUS HOMOGÈNE 212
A. Les propositions de lois de 2005 : l'amorce d'une protection plus large 213
B. Les espoirs nourris par le *Personal Data Privacy and Security Act of* 2009 215
1. Les obligations en matière de traitement des données 216
a. Une obligation de transparence strictement encadrée 216
b. L'obligation de mise en place d'un programme de sécurité des données 217
2. La reconnaissance d'un droit d'accès et de correction 218
3. Les sanctions 219
Conclusion du Chapitre 1 221

CHAPITRE SECOND : DES LOIS ANTI-*SPAM* PARTIELLEMENT INADAPTÉES AUX SPÉCIFICITÉS DU *SPAMMING* 222

SECTION PRÉLIMINAIRE. LE CHOIX ENTRE DEUX RÉGLEMENTATIONS DES ENVOIS COMMERCIAUX, REFLET D'UNE CONCEPTION DUALISTE DU *SPAMMING* 223
§ 1. L'*OPT-IN* : LA PRIORITÉ CONFÉRÉE À UNE PROTECTION FORTE DES « SPAMMÉS » 223
§ 2. L'*OPT-OUT* : LA PRÉFÉRENCE ACCORDÉE AUX INTÉRÊTS ÉCONOMIQUES 224
SECTION I. EN FRANCE, UNE PROHIBITION DE PRINCIPE 226
§ 1. L'HÉRITAGE D'UNE ÉVOLUTION COMMUNAUTAIRE HÉSITANTE 226
§ 2. LE RÉGIME DE L'*OPT-IN* 229
A. Le principe du consentement préalable 230
1. Un champ d'application trop restrictif à certains égards 231
a. La notion légale de courrier électronique 231
b. Les destinataires, personnes physiques 233
c. Des messages à finalité exclusivement commerciale 234
2. Les conditions de régularité des envois commerciaux 236
a. L'exigence de transparence des envois 237
i. Les qualités du consentement préalable 237
ii. Les modalités de recueil du consentement 238
b. Le droit d'opposition renforcé 241
B. Les exceptions au principe de l'*opt-in* 242
1. L'hypothèse des relations commerciales préexistantes 242
2. L'hypothèse des adresses professionnelles 245
C. Un volet pénal inexploité et d'application limitée 246
§ 3. L'ÉCHEC D'UNE LUTTE GLOBALE CONTRE LE *SPAMMING* 247
SECTION II. AUX ÉTATS-UNIS, UNE AUTORISATION DE PRINCIPE 250
§ 1. UNE PROHIBITION LIMITÉE AUX PRATIQUES FRAUDULEUSES OU TROMPEUSES 254

A. L'exigence de transparence des envois 255
B. L'interdiction d'envoi après l'opposition du destinataire 257
C. Les exceptions au régime de l'*opt-out* 259
§ 2. LES RESPONSABILITÉS ET SANCTIONS 260
A. Les hypothèses de responsabilité 260
1. L'hypothèse des expéditeurs multiples 261
2. L'intervention accessoire d'un tiers 263
3. Le mécanisme du « *Forward-to-a-Friend Email Marketing Campaigns* » 263
B. Les sanctions 265
a. Les sanctions administratives 266
b. Les sanctions civiles 266
c. Les sanctions pénales 267
Conclusion du Chapitre 2 269
Conclusion du Titre 2 271
Conclusion de la Partie 1 274

***SECONDE PARTIE LE DÉPASSEMENT NÉCESSAIRE DE LA PROTECTION SPÉCIALE*.276**

TITRE PREMIER : LA RECHERCHE D'UNE ACTION EN RESPONSABILITÉ EFFICACE CONTRE LES « SPAMMEURS » 279

CHAPITRE PREMIER : L'ACTION EN RESPONSABILITÉ PÉNALE 280

SECTION I. LE *SPAMMING*, UNE INFRACTION AUTONOME 281
§ 1. LE *SPAMMING* SANCTIONNÉ POUR INTRUSION DANS UN SYSTÈME 282
§ 2. LE *SPAMMING* SANCTIONNÉ POUR PERTURBATION DU FONCTIONNEMENT D'UN SYSTÈME 287
SECTION II. LE *SPAMMING*, VECTEUR DE MULTIPLES INFRACTIONS 293
§ 1. LE *SPAMMING*, VÉHICULE D'ESCROQUERIES 293
A. Les éléments constitutifs de l'escroquerie 294
1. Condition préalable : le bien susceptible d'escroquerie 295
2. L'élément matériel 296
a. L'acte de tromperie 296
b. La remise du bien 301
c. Le préjudice 302
3. L'élément moral 302
B. Sanctions 303
§ 2. LE *SPAMMING,* VÉHICULE D'INFRACTIONS ISSUES DU DROIT PÉNAL DE LA CONSOMMATION 303
A. La notion de pratique commerciale et ses implications 306
B. Le *spamming* au service des pratiques commerciales trompeuses 310
1. Les tromperies par action 311
a. La confusion 311
b. Les allégations fausses ou de nature à induire en erreur 312

c. L'incertitude quant l'annonceur 314
2. Les tromperies par omission 314
3. Élément moral commun aux pratiques trompeuses 315
4. Poursuites et sanctions 317
C. Le *spamming*, support des pratiques agressives 319
§ 3. LE *SPAMMING,* VÉHICULE D'INFRACTIONS SANCTIONNÉES PAR LE DROIT PÉNAL DE L'INFORMATIQUE 320
Conclusion du Chapitre 1 323

CHAPITRE SECOND : L'ACTION EN RESPONSABILITÉ CIVILE 324

SECTION I. LE *SPAMMING*, GÉNÉRATEUR DE RESPONSABILITÉ DÉLICTUELLE 325
§ 1. L'EXPÉRIENCE AMÉRICAINE COMME PISTE DE RÉFLEXION 326
A. Le *trespass to chattels,* une structure proche du régime de responsabilité français 326
B. Le processus d'adaptation dans le contexte de l'internet 327
1. L'amorce 328
2. L'application du *trespass to chattels* au *spamming* 329
§ 2. L'OPPORTUNITÉ D'UN RECOURS PLUS FRÉQUENT À LA RESPONSABILITÉ DÉLICTUELLE EN MATIÈRE DE *SPAMMING* ? 330
A. La question du comportement fautif du « spammeur » 331
1. La faute en droit positif et ses applications au *spamming* 331
2. L'appréciation de la faute du « spammeur » par les cours américaines 333
B. La question du dommage causé par le *spamming* 335
1. Le dommage en droit positif et ses applications au *spamming* 335
2. Les caractère du dommage réparable 338
3. L'appréciation du dommage par les cours américaines 342
C. La question du lien de causalité en matière de *spamming* 345
D. La question de la réparation des « spammés » 349
1. Le principe de réparation intégrale 349
2. Les limites de l'action en responsabilité délictuelle 356
§ 3. LE *SPAMMING,* UNE OCCASION DE REPENSER UN DROIT DE LA RESPONSABILITÉ CIVILE PLUS ADAPTÉ 358
A. L'opportunité d'introduire la faute lucrative 358
1. Définition et transposition à l'hypothèse du *spamming* 359
2. La nécessité d'une reconnaissance officielle 360
3. La sanction de la faute lucrative : l'opportunité d'introduire des dommages-intérêts punitifs 364
a. Une réception controversée 365
b. La question du régime des dommages-intérêts punitifs 369
B. L'opportunité de consacrer une action de groupe 375
1. La nécessaire prise en compte des dommages de masse par le droit français 377
2. L'opportunité de recourir à la *class action* en cas de dommages de masse 378

3. Analyse critique et prospective de l'introduction de la *class action* en droit français 381

a. La recevabilité de l'action de groupe 382

b. L'action en responsabilité engagée par le représentant 385

c. Le jugement de la *class action* 386

SECTION II. LE *SPAMMING*, GÉNÉRATEUR DE RESPONSABILITÉ CONTRACTUELLE 389

Conclusion du Chapitre 2 395

Conclusion du Titre 1 397

TITRE SECOND : L'ABANDON NÉCESSAIRE D'UNE LOGIQUE NATIONALE : LES MÉRITES DU DROIT INTERNATIONAL PRIVÉ 399

CHAPITRE PREMIER : LES JUSTIFICATIONS DU RECOURS AU DROIT INTERNATIONAL PRIVÉ 402

SECTION I. UN FLÉAU SANS FRONTIÈRES : L'INTERNATIONALITÉ DU *SPAMMING* 403

§ 1. LE *SPAMMING*, UN DÉLIT PLURILOCALISÉ 403

§ 2. LES SPÉCIFICITÉS DU *SPAMMING* 404

SECTION II. À LA RECHERCHE D'UNE RÉPONSE JURIDIQUE GLOBALE 407

§ 1. LES INSTANCES INTERNATIONALES : UNE ACTION INSUFFISANTE 407

§ 2. L'EMPRUNT NÉCESSAIRE AUX MÉCANISMES DE DROIT INTERNATIONAL PRIVÉ 410

Conclusion du Chapitre 1 412

CHAPITRE SECOND : LES APPLICATIONS DU DROIT INTERNATIONAL PRIVÉ EN MATIÈRE DE *SPAMMING* 413

SECTION PRÉLIMINAIRE. LA QUESTION DE LA QUALIFICATION EN MATIÈRE DE *SPAMMING* 417

SECTION I. LES CONFLITS DE JURIDICTIONS SUSCITÉS PAR LE *SPAMMING* 419

§ 1. LE « SPAMMEUR » RÉSIDANT DANS L'UNION EUROPÉENNE 419

A. Le *spamming* soumis à la réglementation communautaire 420

B. L'application du règlement en matière de *spamming* 421

1. Les règles de compétence 422

2. Une mise en pratique délicate 423

§ 2. LE « SPAMMEUR » RÉSIDANT HORS DE L'UNION EUROPÉNNE 429

A. Les règles ordinaires de principe 429

B. La règle de compétence subsidiaire 431

§ 3. PROPOSITIONS D'UN NOUVEAU CRITÈRE DE RATTACHEMENT 432

SECTION II. LES CONFLITS DE LOIS OCCASIONNÉS PAR LE *SPAMMING* 437

§ 1. LA LOI APPLICABLE AUX DÉLITS COMMIS PAR LES « SPAMMEURS » 437

A. L'application du règlement Rome II au *spamming* 438

B. La mise en œuvre du règlement en matière de *spamming* 441

1. Un rattachement de principe : la loi du lieu du dommage 442

2. Un rattachement dérogatoire exceptionnel : la clause d'exception 445

§ 2. LA LOI APPLICABLE EN MATIÈRE D'ATTEINTES AUX DROITS DE LA PERSONNALITÉ DES « SPAMMÉS » 448

A. La mise en œuvre de la règle de conflit française 449

B. La recherche d'un nouveau critère stable de rattachement 451

Conclusion du Chapitre 2 454
Conclusion du Titre 2 456
Conclusion de la Partie 2 458

CONCLUSION GÉNÉRALE **.....460**

BIBLIOGRAPHIE **.....471**

GLOSSAIRE **.....535**

INDEX **.....543**

PLAN DÉTAILLÉ **.....553**