UNIVERSITÉ DE STRASBOURG

ÉCOLE DOCTORALE DROIT, SCIENCE POLITIQUE ET HISTOIRE - ED101

Laboratoire de Recherche du CEIPI – UR 4375

THÈSE

présentée par :

Déborah HERTZ

soutenue le : **13 novembre 2024**

pour obtenir le grade de : **Docteur de l'université de Strasbourg**

Discipline / Spécialité : Science juridique – Droit privé (DR7P61)

Le cadre normatif des données : une construction idéaliste ?

THÈSE dirigée par :

M. MACREZ Franck	Maître de conférences à l'Université de Strasbourg

RAPPORTEURS :

Mme DEBET Anne	Professeure à l'Université de Paris Descartes
M. DOUVILLE Thibault	Professeur à l'Université de Caen Normandie

---

AUTRES MEMBRES DU JURY :

Mme BERTRAND Brunessen	Professeure à l'Université de Rennes
M. DELTORN Jean-Marc	Professeur au CEIPI
M. NETTER Emmanuel	Professeur à l'Université de Strasbourg

L'Université de Strasbourg n'entend donner aucune approbation, ni improbation aux opinions émises dans cette thèse. Ces opinions doivent être considérées comme propres à leurs auteurs.

Remerciements

Tout d'abord, je remercie mon directeur de thèse Monsieur Franck Macrez d'avoir accepté de me suivre dans ce parcours, pour sa patience et ses précieux conseils. Je remercie également l'ensemble de mes membres du jury que sont Mesdames les professeures Brunessen Bertrand et Anne Debet et Messieurs les professeurs Thibault Douville, Emmanuel Netter et Jean-Marc Deltorn.

Je remercie l'amour de ma vie de m'avoir soutenue depuis le premier jour de notre rencontre, d'avoir fait de mon projet le nôtre et d'avoir rendu le chemin chaque jour plus agréable à tes côtés.

Je remercie mes parents d'avoir accepté ces longues études, à Dimitri pour ses conseils avisés et à Stan pour l'insouciance de nos moments. Merci également à ma belle-famille pour leur bienveillance.

Je remercie mes meilleures amies pour leur présence à chaque instant, Sophie depuis toujours, Carla depuis bien longtemps et Elodie depuis nos débuts à l'Université.

Je remercie également mes ami(e)s pour leur soutien particulier lors de ce parcours, Olivier pour ta sagesse, Salomé pour ta persévérance, Hicham pour avoir rendu le professionnel plus agréable. Sans oublier Garin, Marine, Emma et Daviane.

Je remercie enfin, tous les membres du laboratoire du CEIPI.

Liste des abréviations

ADFA	Association française pour la recherche en droit administratif
AFCDP	Association française des correspondants à la protection des données à caractère personnel
Aff.	Affaire
AFNOR	Association française de normalisation
AJ	Actualité juridique
AJCT	Actualité juridique des collectivités territoriales
AJDA	Actualité juridique de droit administratif
API	*Application programming interface*
ARCEP	Autorité de régulation des communications électroniques, des postes et de la distribution de la presse
ARCOM	Autorité de régulation de la communication audiovisuelle et numérique
Art.	Article
CCE	Communication commerce électronique
CEIPI	Centre d'études internationales de la propriété intellectuelle
CEPD	Comité européen de la protection des données à caractère personnel
CEPRISCA	Centre de droit privé et de sciences criminelles d'Amiens
CESE	Comité économique, social et environnemental
CGU	Conditions générales d'utilisation
CGV	Conditions générales de vente
Chron.	Chronique
CJCE	Cour de justice des communautés européennes
CJUE	Cour de justice de l'Union européenne
CNIL	Commission nationale de l'informatique et des libertés
CNNUM	Conseil national du numérique
CNRS	Centre national de la recherche scientifique
CNRTL	Centre national de ressources textuelles et lexicales
CPI	Code de propriété intellectuelle
CRPA	Code des relations entre le public et l'administration
CRU	Conseil de résolution unique
CSA	Conseil supérieur de l'audiovisuel
CSPLA	Conseil supérieur de la propriété littéraire et artistique
CURAPP	Centre universitaire de recherche sur l'action publique et la politique
(dir.)	Sous la direction de
D.	Recueil Dalloz
D. aff.	Revue Dalloz affaires
DA	*Data Act*
Dalloz IP/IT	Dalloz droit de la propriété intellectuelle et du numérique
DC	Décision de conformité
DDHC	Déclaration des droits de l'homme et du citoyen
Déf.	Définition
DGA	*Data governance act*
DGCCRF	Direction générale de la concurrence, de la consommation et de la répression des fraudes
DINUM	Direction interministérielle du numérique
Dir.	Directive

DMA	*Digital Market Act*
DPO	*Data protection officer*
DSA	*Digital Service Act*
éd.	Éditions
EMS	Éditions management et société
ENISA	Agence de l'Union européenne pour la cybersécurité
et s.	et suivantes
FAI	Fournisseur d'accès internet
G29	Groupe de travail de l'article 29
GAFA	Google Amazon Facebook Apple
GAFAM	Google Amazon Facebook Apple Microsoft
Gaz. Palais	Gazette du Palais
GDPR	*General Data Protection Regulation*
HADOPI	Haute autorité pour la diffusion des œuvres et la protection des droits sur Internet
IA	Intelligence artificielle
Ibid.	*Ibidem*
IDFRights	*Institute for Digital Fundamental Rights*
In	dans
Infra	ci-dessous
INSEE	Institut national de la statistique et des études économiques
IoT	*Internet of Things*
IP (address)	*Internet Protocol*
JCP E	La Semaine juridique, édition Entreprise
JCP G	La Semaine Juridique, édition Générale
JDSA	Journal droit et santé et de l'assurance maladie
JO	Journal officiel
JOEU	Journal officiel de l'Union européenne
JORF	Journal officiel de la République française
LCEN	Loi pour la confiance dans l'économie numérique
LGDJ	Librairie générale de droit et de jurisprudence
LIL	Loi informatique et libertés
LPA	Les petites affiches
LRN	Loi pour une République numérique
MAC (adress)	*Media access control*
n°	Numéro
NFIC	Nouvelles technologies de l'information et de la communication
NIR	Numéro d'inscription au répertoire
not.	Notamment
NOYB	*None of your business*
obs.	Observations
OCDE	Organisation de coopération et de développement économique
op. cit.	*Opus citatum*
p.	page
PME	Petites et moyennes entreprises
pp.	pages
préc.	précité
PSI	Directive sur la réutilisation des informations du secteur public
PUF	Presse universitaire de France
R2PI	Podcast de la propriété intellectuelle

RAE	Revue des affaires européennes
RDC	Revue des contrats
RDI	Revue de droit immobilier
RDIA	Revue de droit international d'Assas
RDJA	Revue jurisprudence de droit des affaires
RDLF	Revue des droits et libertés fondamentaux
RDP	Revue du droit public
RDTI	Revue du droit des technologies et de l'information
Rev. UE	Revue de l'Union européenne
RFAP	Revue française d'administration publique
RFDA	Revue française de droit administratif
RFPI	Revue francophone de la propriété intellectuelle
RGPD	Règlement général sur la protection des données
RLDA	Revue Lamy droit des affaires
RLDC	Revue Lamy droit civil
RLDI	Revue Lamy droit de l'immatériel
RPPI	Revue pratique de la prospective et de l'innovation
RTD civ.	Revue trimestrielle de droit civil
RTD com.	Revue trimestrielle de droit commercial
RTD eur.	Revue trimestrielle de droit européen
s.	suivant
SFDI	Société française de droit international
SIA	Système d'intelligence artificielle
SNDS	Système national des données de santé
spéc.	spécialement
SREN	Loi visant à sécuriser et à réguler l'espace numérique
supra.	ci-dessus
TFUE	Traité sur le fonctionnement de l'Union européenne
TGI	Tribunal de grande instance
TI	Tribunal d'instance
TIC	Technologies de l'information et de la communication
TJ	Tribunal judiciaire
TUE	Tribunal de l'Union européenne
UE	Union européenne
v.	voir
VECAM	Citoyenneté dans la société numérique
WWW	*World wide web*

Sommaire

PARTIE 1 : L'ÉLABORATION D'UN CADRE NORMATIF COMPLEXE

TITRE 1 : La diversité évolutive des notions

Chapitre 1 : La notion de données et les notions voisines : divergences et convergences

Chapitre 2 : La notion juridique de données : forces et faiblesses

TITRE 2 : L'excessive diversité des normes

Chapitre 1 : L'établissement d'un cadre ambivalent pour les données

Chapitre 2 : L'émergence d'un cadre concurrentiel pour les données

PARTIE 2 : LA MISE EN ŒUVRE LACUNAIRE DU CADRE NORMATIF

TITRE 1 : L'articulation artificielle des normes

Chapitre 1 : Le modèle pyramidal pour le droit des données : une vision archaïque

Chapitre 2 : Le modèle du réseau de normes pour les données : un outil de subversion

TITRE 2 : L'effectivité limitée des normes

Chapitre 1 : Les limites de l'effectivité des règles

Chapitre 2 : Les limites de l'effectivité des sanctions

INTRODUCTION GÉNÉRALE

> *« La Toile est multiforme. Elle vit sur un Internet que nous souhaiterions le plus neutre possible. Elle est omniprésente. […] Nous sommes nombreux à partager la nostalgie du monde romantique, idéaliste, anarchiste, anarchique, de la Toile ouverte des débuts. La Toile évolue inexorablement vers des espaces plus fermés notamment sous la pression de la monétarisation des contenus. Elle reste à la fois la plus belle des dentelles, le tissu de toutes les connaissances humaines et le terreau des plus horribles fantasmes, de toutes les violences. Elle est aussi l'univers d'une croissance arrogante dans ses imprécisions et ses incohérences qui noient les perles de l'humanité, et d'une alchimie improbable qui transforme la masse en qualité*[1]*. »*

1. L'indépendance utopique. La Toile est un espace déterritorialisé, dématérialisé et caractérisé par l'absence de frontière. L'histoire d'Internet débute dans les années 1960 avec l'idée d'un réseau informatique permettant aux utilisateurs de communiquer grâce à plusieurs ordinateurs. La popularisation de ce réseau date de la fin des années 1980 avec l'apparition du *World Wide Web*, fondé par Tim Bernes Lee. L'apparition d'Internet constitue alors un continent nouveau « mêlé de pensée et d'électrons, dans un à-côté, un ailleurs, un au-delà[2] ». Le 8 février 1996, John Barlow rédige sur cette Toile la « Déclaration d'indépendance du cyberespace » en réaction au « Telecommunication Act » ratifié la veille par la Maison Blanche, visant à censurer certains contenus injurieux et pornographiques[3]. John Barlow s'adresse aux gouvernements avec les propos suivants : « Au nom de l'avenir, je vous demande, à vous qui êtes du passé, de

---

[1] Abiteboul Serge, *Sciences des données : de la logique du premier ordre à la Toile*, éd. Fayard, 2012, p. 101.

[2] Netter Emmanuel, *Numérique et grandes notions du droit privé*, éd. CEPRISCA, 2019, p. 9.

[3] Federal Communications Commission : « The Telecommunications Act of 1996 is the first major overhaul of telecommunications law in almost 62 years. The goal of this new law is to let anyone enter any communications business - to let any communications business compete in any market against any other. The Telecommunications Act of 1996 has the potential to change the way we work, live and learn. It will affect telephone service - local and long distance, cable programming and other video services, broadcast services and services provided to schools. ».

nous laisser tranquilles. Vous n'êtes pas les bienvenus parmi nous. Vous n'avez aucun droit de souveraineté sur nos lieux de rencontre. […] Le cyberespace ne se situe pas dans vos frontières. Ne pensez pas que vous pouvez le construire[4]. ». Il affirme que les gouvernements n'ont pas eu le « consentement des gouvernés » pour établir des lois régissant la Toile. Il avance que ce nouveau monde est ouvert à tous et ne doit être dominé par personne : il s'agit d'un espace protégé de toute régulation ou d'une éventuelle appropriation par un gouvernement extérieur.

2. Une privatisation réaliste. À ce jour, la déclaration de John Barlow demeure le texte fondateur d'une véritable utopie numérique. Un quart de siècle après sa proclamation, la Déclaration d'indépendance du cyberespace « ressemble à la lumière d'une étoile morte, témoin de quelque chose qui brilla mais ne sera plus[5] ». En réalité, la Toile a rapidement été privatisée par quelques entreprises disruptives du numérique ayant établi un ordre décentralisé et asymétrique[6]. Ils dominent la plupart des services du numérique et détiennent une hégémonie impressionnante sur les données. De 1990 à 2010, leurs pratiques sont restées impunies leur permettant d'établir une domination sans précédent sur les données[7]. La possession massive des données de leurs utilisateurs permet à ces acteurs de détenir une situation de monopole, voire d'oligopole en ce domaine[8]. Le dessein d'un monde ouvert à tous sans privilège dicté par

---

[4] Barlow John Perry, « Déclaration d'indépendance du cyberespace », Davos, 8 février 1996 : « Gouvernements du monde industriel, géants fatigués de chair et d'acier, je viens du cyberespace, nouvelle demeure de l'esprit. […] Nous créons un monde où tous peuvent entrer, sans privilège ni préjugé dicté par la race, le pouvoir économique, la puissance militaire ou le lieu de naissance. ».

[5] Patino Bruno, *La civilisation du poisson rouge*, éd. Grasset, 2020, p. 44.

[6] Soumia Malinbaum « Origine libertaire d'Internet et tendance à l'ubérisation des secteurs régulés », *in* Frison-Roche Marie-Anne et Benzoni Laurent (dir.), *Internet, espace d'interrégulation*, éd. Dalloz, 2016, p. 75.

[7] Il faut également rajouter que ces entreprises ont bénéficié d'investissements massifs de l'État pour le développement des technologies émergentes, à ce sujet v. Thibout Charles, « Les GAFAM et l'État : réflexion sur la place des grandes entreprises technologiques dans le champ du pouvoir », Revue internationale et stratégique, 2022 : « Il s'agit là, en quelque sorte, du soutien infrastructurel apporté par l'État à ces entreprises, auquel il faudrait superposer les dégrèvements fiscaux, la mise en place d'un cadre juridique et de mesures de régulation allégées, une législation particulièrement propice à l'éclosion de ce type d'entreprises, telle que le Bayh-Dole Act, l'extension du domaine de la brevetabilité aux logiciels, l'autorisation accordée aux universités de vendre des licences pour les "produits" de la recherche financée sur fonds public. ».

[8] Smyrnaios Nikos, « Les GAFAM, entre emprise structurelle et crise d'hégémonie », Pouvoirs, n° 18, 2023, pp. 19-30 : « La libéralisation des marchés en Europe et en Amérique du Nord a créé un contexte favorable à l'accroissement du pouvoir de marché des acteurs oligopolistiques d'internet et aux pratiques anticoncurrentielles afférentes : érection des barrières à l'entrée technologiques, vente liée forcée, revendication abusive de protection de la propriété industrielle et intellectuelle, non-interopérabilité, etc. […] Le manque de volonté politique de la part des instances régulatrices et les faibles moyens dont elles

un pouvoir économique est vain. Désormais, leurs intentions sont devenues funambulesques, telles que devenir les maîtres de l'industrie spatiale ou encore de faire de leur société le « troisième hémisphère du cerveau[9] ».

Depuis plusieurs années, l'expansion considérable de la masse de données leur a permis d'établir un véritable empire sur cette matière première (I), nécessitant l'élaboration d'un cadre normatif afin de tenter de les réguler (II). L'analyse critique de la construction du cadre normatif et de ses caractéristiques constitue l'objet de cette thèse.

I. L'expansion de la production des données

3. Production des données. Le champ de production des données n'a jamais été aussi vaste et leur volume en constante augmentation (A). Les données sont majoritairement détenues par les géants du numérique, possédant une hégémonie sur cette matière première (B).

A) De la donnée aux données

4. L'existence des données. Tout d'abord, la notion de donnée n'est pas nouvelle : elle est inhérente au vivant. De manière générale, une donnée peut être définie comme une représentation d'une information, permettant aux êtres vivants ou aux systèmes de traiter, interpréter et interagir avec leur environnement. En effet, les êtres humains et les autres formes de vie produisent et consomment des données pour communiquer et s'adapter au monde extérieur. Toutefois, il est pertinent de distinguer les données « naturelles », résultant de phénomènes biologiques ou environnementaux et les données « produites » intentionnellement par les êtres humains[10]. Les données « naturelles » peuvent être des hormones échangées entre organes ou des signaux électriques véhiculées par le système nerveux. L'ensemble de ces données sont naturellement produites par l'homme afin de garantir l'équilibre de son vivant.

---

disposaient ont abouti à ce que les sanctions éventuelles arrivent souvent trop tard ou que les litiges soient résolus par des compromis indolores. ».

[9] Bourdin Aymeric, *Le numérique : locomotive de la 3e révolution industrielle ?*, éd. Ellipses, 2013, p. 6 cité par Lequette Suzanne, *Droit du numérique*, éd. LGDJ, 2024, p. 21 ; Filloux Frédéric, Titre de l'article l'Express : « Les GAFAM, futurs maîtres de l'industrie spatiale », 2021.

[10] Bessot David, Billard Pierre, Bourgeois Matthieu *et al*., « L'empreinte de la donnée sur le vivant : Essai pour un numérique responsable », Rapport, 2024.

Quant aux données « produites » intentionnellement par l'homme, il s'agit de l'écriture, du langage, et plus récemment, des données numériques.

5. La circulation des données. Dans l'histoire de la production et de la transmission des données humaines, l'imprimerie a marqué une étape importante. Avec l'avènement de l'informatique, la donnée numérique est apparue, reposant sur un format binaire, nécessitant une alimentation électrique et permettant de transformer les informations en un langage universel compréhensible par les machines. Là où l'imprimerie avait permis de consigner et de transmettre la mémoire humaine, l'informatique permet non seulement de stocker des informations, mais également de les traiter en temps réel, ouvrant la voie à la mise en réseau des machines et à la circulation instantanée des données.

Avec le développement d'Internet et l'utilisation généralisée du protocole IP, la production, la collecte et la transmission des données numériques ont connu une croissance exponentielle[11]. La croissance exponentielle et la mise en réseau du monde soulèvent des problématiques concernant la régulation des données, les rapports de souveraineté ou encore de gouvernance d'Internet. Par ailleurs, si la mise en réseau permet une collecte massive de données, elle impose de nouveaux outils pour leur exploitation. En effet, la collecte ne suffit pas en soi : les outils d'analyse numérique se sont considérablement développés, bouleversant notre rapport au temps en introduisant la notion de « temps réel ». Les différents capteurs intégrés dans nos outils du quotidien permettent aujourd'hui de collecter les données en temps réel, c'est-à-dire à chaque instant, voire à chaque fraction de seconde. Grâce à la mise en réseau, les individus sont désormais interconnectés en permanence et leurs données sont captées, intégrées et interprétées par différents acteurs en continu. L'interconnexion des individus a pour conséquence une certaine « omniconnexion » des individus.

6. Explosion du volume des données. Le nouveau paradigme technique et social, qualifié d'« omniconnexion », a provoqué une explosion sans précédent de la production des données. En janvier 2024, il existait 5,35 milliards d'internautes dans le monde, soit 66 % de la

[11] v. par exemple, Babinet Gilles et Orsenna Erik, *Big Data, penser l'homme et le monde autrement*, éd. Le Passeur, 2015, p. 20.

population mondiale[12]. L'essor du nombre d'internautes augmente *de facto* le nombre de données numériques produites dans le monde entier[13]. La majorité de la population mondiale utilise quotidiennement des services numériques tels que le moteur de recherche, service encore inexistant il y a une trentaine d'années[14]. En parallèle, les capteurs dispersés dans la vie publique ou privée contribuent à la numérisation en temps réel d'une quantité considérable de données sur nos activités[15] : le champ de production des données n'a jamais été aussi vaste. La masse de données double tous les deux ans et devait déjà atteindre 44 zettaoctets en 2020[16]. En 2025, le volume devrait atteindre 180 zettaoctets, un volume dont la quantification relève de l'irrationnel[17]. La croissance vertigineuse du volume de données est communément caractérisée par l'appellation « Big Data ».

7. Le phénomène de « Big Data ». La notion de « Big Data » est apparue dans les années 2010 et désigne en français les « mégadonnées » ou « données massives »[18]. En réalité, il s'agit d'une notion non quantifiable, résultant d'un phénomène pratique ne permettant pas d'en

---

[12] Statista, « Nombre d'utilisateurs internet et des réseaux sociaux dans le monde en janvier 2024 », disponible en ligne sur : https://fr.statista.com/statistiques/1350675/nombre-utilisateurs-internet-reseaux-sociaux-monde/.

[13] Rouvroy Antoinette, « Des données sans personne: le fétichisme de la donnée à caractère personnel à l'épreuve de l'idéologie des Big Data », 2014 : « Parcourue par des logiques de flux et de valorisation des flux, notre époque serait marquée ou se démarquerait - si l'on peut dire - par une « explosion » des volumes de données numériques, reflétant le monde jusque dans ses moindres événements sous une forme éclatée, segmentée, distribuée, décontextualisée, déhistoricisée, ou, pour le dire autrement, sous forme de données individuellement a-signifiantes mais quantifiables, opérant comme de purs signaux en provenance du monde connecté, métabolisables à grande vitesse par les systèmes informatiques. ».

[14] Frenot Stéphane, Grumbach Stéphane, « Des données à l'intermédiation, une révolution économique et politique. Big data : nouvelles partitions de l'information », *in* Broudoux Evelyne et Chartron Ghislaine (dir.), *Big data, Open data. Quelles valeurs ? Quels enjeux ?*, éd. de Boeck, 2014, pp. 97-120.

[15] Bergé Jean-Sylvestre et Grumbach Stéphane, « La sphère des données et le droit : nouvel espace, nouveaux rapports aux territoires », Journal du droit international, 2016, n° 4, pp. 1153-1173.

[16] Basdevant Adrien et Mignard Jean-Pierre, *L'empire des données*, éd. Don Quichotte éditions, 2018, p. 10 ; « La quantité de données croit exponentiellement, suivant une loi similaire à la Loi de Moore, qui avait prédit en 1965 le doublement de la capacité des ordinateurs tous les 18 mois. » ; Un zettaoctet est équivalent à un sextillion d'octets, soit précisément 1 000 000 000 000 000 000 000 d'octets.

[17] Statista, « Le Big Bang du Big Data », 2021 : « En comparant avec des éléments plus tangibles, cela signifie qu'il faudrait se procurer 640 millions des plus gros disques SDD actuellement commercialisés (100 To de stockage) pour être en mesure de sauvegarder les 64 zettaoctets de données générées en 2020. », disponible en ligne sur : https://fr.statista.com/infographie/17800/big-data-evolution-volume-donnees-numeriques-genere-dans-le-monde/.

[18] Journal Officiel de la République Française (JORF), n° 0193, 2014, définition de « Données massives » ayant comme équivalent étranger « Big Data » : « Données structurées ou non dont le très grand volume requiert des outils d'analyse adaptés. ».

donner une définition unique[19]. Il convient toutefois de distinguer « le Big Data » et « les big data » : au singulier la notion correspond à un phénomène, c'est-à-dire au traitement et à l'exploitation des données par des algorithmes tandis que le pluriel représente l'agrégat massif de données. Le *Big Data* est caractérisé par la formule des « 5V » c'est-à-dire volume, vélocité, variété, valeur et véracité.

Le volume représente l'augmentation de la masse de données. Le volume des *big data* correspond à la détention des données directement utiles, des données dont l'utilité a déjà été consommée ou encore des données potentiellement utiles. L'essentiel du *Big Data* est caractérisé par la quantité des données et non forcément l'utilité des données[20] : l'utilité des données pourra être déterminée par des usages secondaires. La vélocité renvoie à la vitesse du traitement permettant de traiter les données jusqu'au temps réel grâce aux outils d'analyse. Les outils d'analyse vont permettre de corréler les données de façon dynamique[21]. Quant à la variété, cela correspond simplement à la diversité des sources : les données proviennent des données produites par les entreprises, de l'État ou encore des personnes. Le quatrième V de valeur illustre la valeur attendue puisque l'objectif est de créer de la valeur grâce à l'exploitation de cette masse de données[22]. Pour finir, le cinquième V de véracité implique la fiabilité des données. La fiabilité des données est devenue un enjeu majeur de ce phénomène, le manque de véracité pouvant remettre en cause les conclusions[23]. *In fine*, l'essentiel du phénomène repose sur la quantité des données et non leur utilité dans un premier temps[24].

8. Une notion en expansion. L'essor de la quantité des données est un phénomène constant avec la massification de l'informatisation du fait humain et l'omniconnexion des individus[25].

---

[19] Bougeard Aurélien, « Le phénomène de Big Data et le Droit, Pour une appréhension juridique par sa décomposition technique », Thèse, 2022, Strasbourg, p. 79 : « Il s'agit d'un phénomène pratique, global à un espace, qui a de multiples usages et qui est protéiforme, ce qui ne permet pas d'en donner une définition unique facilitant son appréhension dans un tout. ».

[20] Rouvroy Antoinette et Colin Jean-Noël, « Des données et des Hommes. Droits et libertés fondamentaux dans un monde de données massives », Conseil de l'Europe, 2016, p. 5.

[21] Zolynski Célia, « Big data : pour une éthique des données », Information, données & documents, 2015, pp. 25-26.

[22] Brasseur Christophe, *Enjeux et usages du big data*, éd. Lavoisier, 2016.

[23] Conseil d'État, « Le numérique et les droits fondamentaux », étude annuelle, 2014, p. 49.

[24] Rouvroy Antoinette et Colin Jean-Noël, *op. cit*., p. 5.

[25] Schmitt Églantine, « L'ambiguïté épistémologique des big data », *in* Broudoux Éveline et Chartron Ghislaine (dir.), *Big Data - Open Data : Quelles valeurs ? Quels enjeux ?*, éd. De Boeck, 2015.

La masse de données étant exponentielle, il convient de parler « des données » plutôt que de « la donnée » : la donnée isolée n'ayant pas réellement de valeur[26]. Pour la masse, il peut s'agir de « *soft data* » émanant des individus soit intentionnellement soit involontairement provenant d'internet avec les réseaux sociaux et les moteurs de recherche. Il peut également s'agir de « *hard data* » émanant des administrations publiques, de métadonnées ou encore de l'ensemble des données provenant de l'Internet des objets[27]. Les objets connectés pour la maison ou l'individu et la quantification de soi avec les applications de santé constituent de nouveaux vecteurs de production de données[28]. La collecte et l'exploitation de ces données comportent des risques pour la vie privée des individus, souvent inconscients de cette collecte massive. En réalité, le *Big Data* devient le point de rencontre entre la multiplication des données, les besoins d'analyse de ces données et les progrès de la technologie[29]. Le développement de l'intelligence artificielle renforce l'essor du phénomène de *Big Data*.

9. Le phénomène d'intelligence artificielle. Selon l'analyse notionnelle, le terme « intelligence artificielle » est composé de deux mots : l'un renvoie à la capacité de penser et le second signifie produit par l'humain[30]. L'intelligence artificielle désignerait alors un pouvoir de réflexion instauré par les personnes physiques[31]. Le terme a été popularisé par les auteurs John McCarthy et Marvin Lee Minsky en 1956[32] et va être délaissé pendant un certain temps en raison du manque de progrès dans ce domaine. Toutefois, au début du XXIème siècle, la technique va être réappropriée de manière considérable en raison de l'explosion de la masse de

---

[26] Colin Nicolas et Verdier Henri, *L'Âge de la multitude*, éd. Armand Colin, 2012, p. 102 : « Avec le mouvement des big data, nous entrons dans une "société sans secrets". […] La croissance exponentielle du volume des informations personnelles et leur maniabilité accrue constituent le moteur des stratégies de création de valeur fondées sur l'analyse de comportement de la multitude. Il ne sera plus indispensable d'être un créateur de génie, de disposer de l'intuition d'un grand designer ou de maîtriser une plateforme pour pouvoir jouer avec la puissance disponible chez les individus et dans le corps social. ».

[27] Rouvroy Antoinette, « La robotisation de la vie ou la tentation de l'inséparation », *in* De Streel Alexandre, Jacquemin Hervé (dir.), *Intelligence artificielle et droit*, éd. Larcier, 2017, pp. 13-46.

[28] Chignard Simon et Benyayer Louis-David, *Datanomics*, éd. FYP, 2015.

[29] Brasseur Christophe, *op. cit*.

[30] Larousse, v° Artificiel : « Qui est le produit de l'activité, de l'habileté humaine », v° Intelligence : 5. « capacité de saisir une chose par la pensée ».

[31] Ancel Bruno, « L'intelligence artificielle au XXIe siècle : outil juridique fiable ou amplificateur d'injustices ? », LPA, 31 mai 2024.

[32] Castets-Renard Céline, « Quelle politique européenne de l'intelligence artificielle ? », RTD eur., 2021, n° 297.

données et du raffinement des outils d'analyse[33]. Pour un groupe d'experts, il serait possible de définir cette technologie comme « des systèmes logiciels conçus par des humains qui, étant donné un objectif complexe, agissent dans la dimension physique ou numérique en percevant leur environnement par l'acquisition de données[34] ». La dimension humaine représente souvent le dénominateur commun des définitions de l'intelligence artificielle : en effet, l'intelligence artificielle « s'inspire, imite et étend l'intelligence humaine, par la structure ou par ses actions[35] ».

Récemment, une définition légistique de l'intelligence artificielle a été instaurée au niveau européen. Le système d'intelligence artificielle est désormais défini comme « un système automatisé qui est conçu pour fonctionner à différents niveaux d'autonomie et peut faire preuve d'une capacité d'adaptation après son déploiement, et qui, pour des objectifs explicites ou implicites, déduit, à partir des entrées qu'il reçoit, la manière de générer des sorties telles que des prédictions, du contenu, des recommandations ou des décisions qui peuvent influencer les environnements physiques ou virtuels[36] ». En effet, les systèmes dotés d'intelligence artificielle sont capables d'adapter leurs comportements en fonction de leurs actions précédentes. L'essor de l'intelligence artificielle a été permis grâce à la quantité de données disponibles, les progrès en termes de puissance de calcul et le développement de nouveaux algorithmes. Les algorithmes pouvant être définis comme un ensemble de règles définissant de manière précise une séquence d'opérations permettant d'atteindre une solution, de résoudre un problème[37]. En somme, l'intelligence artificielle est une famille de technologies en constante évolution.

---

[33] Derave Charly, Frydman Benoît et Genicot Nathan, *L'intelligence artificielle face à l'État de droit*, éd. Bruylant, 2024, p. 11.

[34] Commission européenne, « Lignes directrices pour une intelligence artificielle de confiance », Direction générale des réseaux de communication, du contenu et des technologies, 2019.

[35] Deltorn Jean-Marc, « Le droit des brevets à l'épreuve de l'intelligence artificielle », Thèse, Strasbourg, 2021, p. 19.

[36] Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle (règlement sur l'intelligence artificielle).

[37] Gillespie Tarleton, « The redevance of Algorithms », *in* Gillespie Tarleton, J. Boczkowki Pablo et A. Foot Kirsten (dir.), *Media Technologies : Essays on Communication, Materiality, and Society*, éd. MIT Press, p. 167 cité par Deltorn Jean-Marc, « Le droit des brevets à l'épreuve de l'intelligence artificielle », Thèse, Strasbourg, 2021, p. 14.

10. Une notion trompeuse. Néanmoins, la notion juridique de l'intelligence artificielle ne fait toujours pas l'objet d'un consensus à l'échelle internationale. Tout d'abord, la notion est entravée par un manque de cohérence au niveau scientifique[38]. Auparavant, plusieurs termes étaient utilisés tels que les systèmes automatisés, les algorithmes ou encore les mégadonnées, sans pour autant prendre en compte l'entièreté de la technologie[39]. Il est difficile de définir de façon générale cette technologie « tant elle renvoie à une réalité polymorphe et multisectorielle[40] ». Pour d'aucuns, le terme d'intelligence artificielle serait erroné et n'existerait pas[41]. En effet, l'intelligence artificielle apparaît comme un oxymore puisque les deux termes sont contradictoires : l'intelligence renvoie à une faculté de penser et le vocable artificiel renvoie à des systèmes informatiques dénués de conscience[42]. Il s'agit donc d'une parfaite contradiction dans la mesure où il est impossible d'être à la fois intelligent et artificiel[43]. Le terme d'intelligence artificielle représenterait un amalgame « aussi riche que nébuleux[44] » puisqu'il faut s'interdire de voir dans les technologies précitées une quelconque intelligence au sens humain, c'est-à-dire une capacité de compréhension semblable à l'humain : les algorithmes

[38] Renondin de Hauteclocque Stanislas, « L'intelligence artificielle : les différents chemins de la régulation », Revue internationale d'éthique sociétale et gouvernementale, 2021.

[39] Merabet Samir, *Vers un droit de l'intelligence artificielle*, éd. Dalloz, 2020, p. 48.

[40] Lequette Suzanne, *Droit du numérique*, éd. LGDJ, 2024, p. 763 : « Suggestion de contenus sur internet, aide au diagnostic médial, création d'œuvre, traitement au langage, aide à la surveillance, conduite autonome d'un véhicule, aide à la décision, à la surveillance, etc. sont autant d'exemples révélant combien l'intelligence artificielle assiste, voire parfois remplace l'homme, selon des modalités variables, dans tous les secteurs de la société. ».

[41] Selon l'INRIA (Institut national de recherche en sciences et technologies du numérique), définition disponible sur : https://www.inria.fr/fr/intelligence-artificielle : « L'intelligence artificielle n'existe pas… mais la puissance combinée de données disponibles, d'algorithmes (souvent fondés par des approches par apprentissage) et de ressources de calcul ouvre de formidables perspectives dans de nombreux domaines. ».

[42] Ancel Bruno, *op. cit*.

[43] Barraud Boris, *Humanisme et intelligence artificielle*, éd. Harmattan, 2022, p. 342 : « L'intelligence repose sur les mécanismes biochimiques des neurones, et donc sur une forme biologique, si bien que sitôt que l'intelligence artificielle deviendrait réellement intelligente (et non plus un simple ensemble de calculs et de statistiques) elle cesserait d'être artificielle. ».

[44] Deltorn Jean-Marc, *op. cit*., p. 13.

exécutent, ils ne pensent pas[45]. En ce sens, il serait préférable d'évoquer une « compétence artificielle » et non une intelligence artificielle[46].

11. Une notion fantasmagorique. En pratique, le terme d' « intelligence artificielle » fait l'objet de nombreux fantasmes évoquant une société de transhumanisme ou encore de « gouvernementalité algorithmique[47]. ». Autour de l'intelligence artificielle, les médias insistent particulièrement sur cet aspect fantasmagorique. Ils répandent l'idéologie selon laquelle l'intelligence artificielle dépasserait les humains dans un avenir proche menaçant l'humanité d'extinction[48]. Par-delà le fantasme, l'image du « juge-robot » ou le développement du crédit social sont des phénomènes rendant certaines dystopies littéraires d'actualité[49]. Les instances européennes ou la doctrine ont déjà évoqué les lois d'Asimov ou encore Frankenstein pour développer un cadre pour l'intelligence artificielle[50]. Par ailleurs, les « robots tueurs » ne sont plus seulement mythiques mais existent dans certains pays. En 2020, un rapport de l'ONU signalait qu'en Lybie, un drone autonome avait pris pour cible de son propre chef des soldats qui battaient en retraite[51].

---

[45] Poullet Yves, *op. cit*., p. 16 : « L'intelligence que nous imputons à nos machines reste une création humaine et trouve sa puissance dans le cerveau humain dont elle est le produit. Les informaticiens soulignent à juste titre que la mise au point des algorithmes, la constitution de mégadonnées, les jeux de test et la supervision nécessaire au fonctionnement de la machine afin qu'elles puissent être autoapprenante sont autant d'actes de l'intelligence humaine et que ce travail représente plus de 90% de ce qui est nécessaire pour le fonctionnement des systèmes de machine learning. ».

[46] Barbé Vanessa et Mauclair Stéphanie, *Intelligence artificielle & droits fondamentaux*, éd. Épitoge, 2022, p. 30 qui cite la Professeure Laurence Devillers.

[47] Poullet Yves, *Le RGPD aux défis de l'intelligence artificielle*, éd. Larcier, 2020, p. 8 ; Le terme de « gouvernementalité algorithmique » provient d'Antoinette Rouvroy : « Gouvernementalité algorithmique et perspectives d'émanticipation. Le disparate comme condition d'individualisation par la relation ? », Réseaux, 2013, n°177.

[48] Lassègue Jean, « Que faut-il entendre par "surveillance" en contexte digital ? », Revue pratique de la prospective et de l'innovation, n° 2, dossier 16, novembre 2021.

[49] Derave Charly, Frydman Benoît et Genicot Nathan, *op. cit*., p. 9 : « Les progrès informatiques en matière d'intelligence artificielle réveillent depuis quelque temps des angoisses profondes relatives à la domination de l'humain par la technique et les machines. » ; Rouvière Frédéric, « Le raisonnement par algorithmes : le fantasme du juge-robot », RTD civ., 2018, 530.

[50] Bensamoun Alexandra et Loiseau Grégoire, « L'intelligence artificielle : faut-il légiférer ? », D., 2017, 581 ; Résolution du Parlement européen adoptée le 16 février 2017 contenant des recommandations à la Commission concernant des règles de droit civil sur la robotique ; Macrez Franck et Dreyfuss Laurence, « Les lois de la robotique d'Asimov et le Droit », RFPI, n° spécial, mars 2020, éditorial, p. 6 : « Les fameuses lois de la robotique édictée par Isaac Asimov dans son cycle des robots constituent bien souvent un modèle de référence, conscient ou non, pour qui veut penser la régulation de l'intelligence artificielle. ».

[51] Barbé Vanessa et Mauclair Stéphanie, *op. cit.*, p. 37.

En réalité, certains débats sur l'intelligence artificielle occultent une série d'enjeux actuels et fondamentaux : la concentration du pouvoir et de nos données par des sociétés privées et notre prédisposition à laisser la charge de décider à des algorithmes conçus par ces entreprises[52].

B) L'hégémonie des géants du numérique sur les données

12. L'économie des données. Au cours de la dernière décennie, les entreprises de technologies ont connu une croissance unique dans l'histoire économique, figurant désormais aux premières places des capitalisations boursières. Parmi les capitalisations boursières les plus importantes au monde figurent Microsoft, Apple, Amazon ou encore Alphabet. Ils représentent ensemble plus de 9 000 milliards de capitalisation et ont réussi à rivaliser avec l'industrie pétrolière, absolument centrale pour l'économie[53]. En 2010, la moitié des dix premières capitalisations mondiales était constituée de pétroliers : il n'en reste qu'un aujourd'hui[54]. Les données ont effectivement remplacé le pétrole, même si la comparaison n'est pas idoine puisque les données sont une ressource inépuisable contrairement au pétrole[55]. À ce jour, ils détiennent 80% des informations personnelles numériques de l'humanité : « Jamais, dans l'histoire de l'humanité, un si petit nombre d'individus aura concentré autant de pouvoirs et de richesses[56]. ». *In fine*, leur modèle repose sur une asymétrie consistant à tout savoir de leurs utilisateurs tandis que l'utilisateur ne doit rien savoir du comportement des plateformes[57]. Le monopole des géants

---

[52] Rouvroy Antoinette, « La robotisation de la vie ou la tentation de l'inséparation », *in* De Streel Alexandre et Jacquemin Hervé (dir.), *L'intelligence artificielle et le droit*, éd. Larcier, 2017, p. 15.

[53] Statista, « La suprématie boursière des Big Tech », en ligne, 7 mars 2024 : « En outre, il faut à l'heure actuelle réunir les cinq entreprises avec les capitalisations boursières les plus importantes d'Europe - Novo Nordisk, le géant du luxe LVMH, le spécialiste européen des semi-conducteurs ASML, la multinationale agroalimentaire Nestlé, ainsi que le groupe Hermès (soit près de 2 000 milliards de dollars) - pour atteindre presque l'équivalent de la valorisation du géant américain des puces Nvidia : environ 2 150 milliards de dollars le 6 mars 2024. Nvidia est actuellement la troisième capitalisation boursière américaine derrière Apple (2 600 milliards de dollars) et Microsoft (près de 3 000 milliards). ».

[54] Jean-Sylvestre Bergé et Stéphane Grumbach, « La sphère des données et le droit : nouvel espace, nouveaux rapports aux territoires », *op. cit*. : « Un seul pétrolier a survécu à cette inversion de tendance si symptomatique du rebond de l'anthropocène : Exxon face à Apple, Alphabet, Microsoft, Facebook, Amazon, Tencent. ».

[55] Nevejans Nathalie, « Données et technologies numériques : quels défis pour le XXIe siècle ? », *in* Nevejans Nathalie (dir.), *Données et technologies numériques*, éd. mare et martin, 2021, p. 15.

[56] Dugain Marc, Labbé Christophe, *L'homme nu. La dictature invisible du numérique*, éd. Robert Laffon, 2016, p. 23.

[57] Wylie Christopher et Blanchard Aurélien*, Mindfuck. Le complot Cambridge Analytica pour s'emparer de nos cerveaux*, éd. Bernard Grasset, 2020.

du numérique sur les données de l'ensemble de la planète comporte des risques pour le respect de la vie privée des individus et des enjeux de régulation des données sans précédent.

13. L'intermédiation. En pratique, il est possible de qualifier leurs services d'intermédiation. En effet, les services novateurs de ces entreprises du numérique consistent à assurer une intermédiation entre les personnes ou avec des services. Par exemple, le moteur de recherche met en relation des personnes avec des connaissances et les réseaux sociaux des personnes avec leur environnement[58]. Les services d'intermédiation reposent sur la même architecture : la récolte des données des utilisateurs. À l'instar du pétrole qui est raffiné, les données sont analysées et traitées afin de produire de la valeur : l'analyse des données permet de développer des nouveaux services toujours plus adaptés. Le système est paradoxalement élémentaire : plus il y a d'utilisateurs, plus les plateformes peuvent récolter de données et plus les services deviennent pertinents[59].

En 2024, plus de 35% du temps total passé sur Internet relève des réseaux sociaux. Facebook est toujours le réseau le plus utilisé dans le monde avec 3 milliards d'utilisateurs, suivi par Youtube et WhatsApp avec 2 milliards. Facebook est un réseau social connu depuis plus d'une dizaine d'années. En revanche, le réseau TikTok a connu une véritable expansion en un temps record. Le réseau est utilisé par 1,5 milliard d'individus dont 80% des utilisateurs vont sur TikTok « pour regarder du contenu drôle et divertissant[60] ». Les données de ces utilisateurs peuvent donc être continuellement récoltées par ces plateformes. Le paroxysme de leur collecte

---

[58] Grumbach Stéphane, *op. cit*.

[59] Bévière-Boyer Bénédicte, « Faire face au risque de souveraineté numérique incontrôlée », Dalloz IP/IT, 2020 : « Théâtres de mise en ligne d'un nombre incalculable d'informations personnelles et professionnelles, ils collectent inlassablement, en continu, les données laissées par les internautes, utilisateurs de leurs produits et services, usagers de leurs messageries et réseaux sociaux. Facebook connaît ainsi les goûts, les sujets de discussion, les opinions politiques des utilisateurs, Amazon, les envies d'achat, les goûts, Google, les recherches d'informations sur les sites consultés, les vidéos consultées sur YouTube, les déplacements (Google Map), les agendas, etc. Même les visages sont intégrés dans des bases de données destinées à être exploitées pour des activités d'identification, de paiement, par le biais de la reconnaissance faciale. Croisées, les données ont d'autant plus de valeur pour leur exploitation, particulièrement dans le domaine de la publicité de plus en plus personnalisée, et pour l'offre de ventes ciblées. De par leur situation de quasi-monopole du stockage des données, en l'absence de tout contrôle, les géants du net sont à l'origine de dérapages multiples. ».

[60] Coëffé Thomas, « Chiffres réseaux sociaux 2024 », disponible en ligne sur : https://www.blogdumoderateur.com/chiffres-reseaux-sociaux/.

des données a été atteint à la fin de l'année 2021, en pleine pandémie de Covid-19[61]. Pendant les confinements successifs, le temps d'écran a été drastiquement augmenté, permettant à ces entreprises de récolter davantage de données et d'atteindre une valeur capitalistique exorbitante[62].

14. Le développement des objets connectés. De surcroît, la croissance exponentielle des objets connectés participe activement à la collecte massive des données. Depuis quelques années se développent des objets « smart » permettant d'améliorer nos intérieurs : brosse à dents intelligente, four intelligent, machine à café intelligente ou encore gourde intelligente. Par exemple, la gourde « smart » de la marque Apple permet de « vous rappeler de boire régulièrement et effectue le suivi de la quantité d'eau que vous buvez » grâce à vos données à caractère personnel[63]. En réalité, ces produits sont totalement absurdes et factuellement inutiles[64]. Inutile pour l'utilisateur mais extrêmement rentable pour les sociétés qui les exploitent. Surtout, les objets connectés permettent de renforcer le capitalisme de surveillance en générant des données sur l'ensemble de notre vie quotidienne. L'avantage concurrentiel de ces sociétés repose sur les données et les capacités algorithmiques de les traiter[65]. Les plateformes ont développé leurs services en s'inspirant des pratiques du casino : le défilement infini et les fonctions addictives destinées à stimuler la zone de récompense du cerveau. Dans les jeux d'argent, les casinos vont gagner de l'argent selon le nombre de tours joués par les individus. Pour les réseaux sociaux, l'argent est gagné en fonction du nombre de clics par

[61] Patard Alexandra, « Étude sur l'usage d'Internet, des réseaux sociaux et du mobile au 1er trimestre 2020 », BDM, 27 avril 2020 : « La pandémie du Covid-19 a bouleversé les comportements numériques ces derniers mois partout dans le monde. Les milliards d'internautes, qui se sont retrouvés confinés pour tenter de lutter contre le virus, se sont tournés vers les médias sociaux et Internet, afin de rester en contact avec leurs proches, s'informer ou encore les aider à travailler depuis leur domicile. ».

[62] Smyrnaios Nikos, *op. cit*., : « En novembre 2021, au pic de la pandémie, les GAFAM ont atteint des taux de marge record : 38 % pour Microsoft, 37 % pour Meta, quasiment 30 % pour Alphabet et plus de 26 % pour Apple. Début décembre, la valeur capitalistique de ce dernier a atteint le plus haut historique jamais enregistré pour une entreprise états-unienne à la somme astronomique de 2 650 milliards de dollars, suivie par celles de Microsoft (2 570 milliards), Alphabet (1 980 milliards), Amazon (1 850 milliards) et Meta (1 000 milliards). Le Nasdaq, indice de valeurs technologiques, a progressé de 64 % en moins de deux ans, entre février 2020 et novembre 2021. ».

[63] Apple, « Gourde connectée HidrateSpark PRO STEEL (945 ml) + bouchon supplémentaire avec paille », site Apple, disponible sur https://www.apple.com/fr/shop/product/HQ212ZM/A/gourde-connect%C3%A9e-hidratespark-pro-steel-945-ml-bouchon-suppl%C3%A9mentaire-avec-paille.

[64] Cousin Olivier, *op. cit*.

[65] Marty Frédéric, « Économie de la donnée. Écosystèmes numériques, algorithmes et intelligence artificielle », *in* Jean-Michel Bruguière, *L'émergence d'un droit des données*, éd. Dalloz, 2023, p. 25.

l'utilisateur. Il existe donc peu de différences entre les pratiques des casinos et celles des réseaux sociaux, à l'exception que les pratiques du casino sont drastiquement encadrées. Pourtant, les réseaux sociaux ne cessent de développer des techniques occultes de manipulation afin de générer des comportements compulsifs, orienter les choix ou tout simplement maintenir l'attention de l'utilisateur[66].

15. L'économie de l'attention. Il ne s'agit plus seulement de collecter l'ensemble des données sur les individus, les plateformes souhaitent désormais maîtriser l'attention de leurs utilisateurs[67]. La « capture attentionnelle » est un prolongement du marché prolifique des acteurs du numérique, leur permettant de récolter davantage de données et de garder le plus longtemps possible l'individu sur leur plateforme[68]. L'économie de l'attention repose sur un alliage entre la collecte et l'exploitation des données, des dispositifs de recommandation de contenus grâce aux algorithmes et des récompenses aléatoires[69]. Le dessein est d'attirer et de conserver l'attention de l'individu, « réduit à sa dimension de prospect, dans l'orbite d'influence des opérateurs susceptibles de monétiser cette attention[70] ». Afin de développer les algorithmes permettant de rentabiliser l'économie de l'attention, les plateformes n'hésitent pas à faire primer la performance économique sur la sécurité des utilisateurs.

16. Promotion des contenus extrêmes. Cette stratégie a été confirmée et documentée par la lanceuse d'alerte Frances Haugen au printemps 2021, divulguant plus de 20 000 pages de documents internes au sujet de la plateforme Facebook. En effet, les contenus haineux ou choquants sont des contenus qui provoquent davantage d'engagement de la part des utilisateurs. De fait, les études internes démontrent que les algorithmes de Facebook et d'Instagram font la promotion de contenus de plus en plus extrêmes au fil du temps afin de gagner les clics et

---

[66] Bertrand Brunessen et Sirinelli Jean, « L'approche comportementale dans la régulation du numérique », *Entre art et technique : les dynamiques du droit : mélanges en l'honneur de Pierre Sirinelli*, éd. Dalloz, 2022, p. 583.

[67] Patino Bruno, *Submersion*, éd. Grasset, 2023, p. 61 : « La compétition effarante pour notre attention a engendré des monstres dont la taille ne cesse de grandir. Chaque heure de notre vie est une cible pour l'ensemble des plateformes. Celles qui vivent de la publicité sont totalement dépendantes du temps qu'on leur consacre. ».

[68] Pineau Karl et Fabre Aurelia, « Évaluer la captologie et le design persuasif des services numériques », Information, données & documents, 2, 2021.

[69] Zolynski Célia, Le Roy Marylou et Levin François, « L'économie de l'attention saisie par le droit », Dalloz IP/IT, 2019, 614.

[70] Benabou Valérie-Laure et Rochfeld Judith, *À qui profite le clic ?*, éd. Odile Jacob, 2015, p. 20.

commentaires des utilisateurs. Pour les plateformes, l'important n'est pas de maximiser la véracité des contenus mais la présence des internautes à travers des contenus engageants[71]. En 2020, le Wall Street Journal révélait qu'un document interne de Facebook reconnaissait que « nos algorithmes exploitent l'attraction du cerveau humain pour la discorde[72] ». L'ordonnancement des contenus soulève des problèmes de modération privée par ces sociétés et est relancé par la propagation des contenus générés par les intelligences artificielles[73].

17. Impact sur les mineurs. Par ailleurs, Facebook n'hésite pas à inciter les mineurs à devenir des utilisateurs de la plateforme afin de récolter davantage de données, même si cela présente des risques pour leur santé. La lanceuse d'alerte a également partagé des entretiens internes avec des mineurs évoquant l'utilisation d'Instagram de façon compulsive. Les chercheurs de Facebook avaient qualifié dans ce document les dires des enfants de « propos de toxicomanes[74] ». L'usage des plateformes par les enfants provoque un impact considérable sur leur santé et leur confiance en soi. Récemment, en avril 2024, un groupe d'experts de la société civile a évalué les effets de l'usage des écrans chez les mineurs dans un rapport intitulé « Enfants et écrans. À la recherche du temps perdu » [75]. Le rapport alerte les pouvoirs publics

---

[71] Abiteboul Serge et Cattan Jean, *Nous sommes les réseaux sociaux*, éd. Odile Jacob, 2022, p. 47 : « L'attention est au cœur du modèle d'affaires des réseaux sociaux. Leur cœur de métier est de faire en sorte que l'on y reste plus longtemps pour nous exposer à des encarts publicitaires. Cela requiert que nous passions toujours plus de temps sur les réseaux, que nous soyons toujours plus nombreux à le faire et que nous communiquions toujours plus de données sur qui nous sommes. ».

[72] Horwitz Jeff et Seetharalan Deepa, « Facebook executives shut down efforts to make the site less divisise », The Wall Street Journal, 26 mai 2020.

[73] Favro Karine, « La lutte contre les stratégies d'influence et les ingérences », *in* Bertrand Brunessen et Le Floch Guillaume (dir.), *La souveraineté numérique*, éd. Bruylant, 2024, p. 208 : « Il est en effet avéré que les "réseaux sociaux définissent un ordonnancement des contenus" qui repose, pour la plupart d'entre eux, sur une logique d'individualisation résultant de l'analyse des données relationnelles issues de l'activité du réseau de l'utilisateur. Ces opérateurs sont alors en capacité d'accélérer ou de ralentir la circulation des contenus, ce qui constitue une forme d'éditorialisation de fait. ».

[74] Haugen Frances, *La vérité sur Facebook*, éd. Fayard, 2024, p. 332 : « L'entreprise disposait d'une pile d'entretiens avec des enfants qui disaient utiliser Instagram de façon compulsive même si cela les rendait malheureux. […] Et pourtant, la réponse de Facebook au congrès n'a guère été plus qu'un haussement d'épaules : "concernant la question de savoir combien de temps passé devant un écran serait "trop", nous n'avons pas connaissance d'un consensus parmi les études ou les experts" a affirmé l'entreprise en esquivant lâchement la question posée. Techniquement, Facebook avait raison de dire qu'il n'y avait pas de consensus dans le monde universitaire ou dans le public sur la question de savoir quelle quantité de réseaux sociaux était "trop". Mais cela s'explique en grande partie par le fait que Facebook dissimule toutes ses données et ne permet pas aux universitaires d'y accéder pour réaliser des études. ».

[75] Mouton Sevane, Benyamina Amine, Bernard Jonathan, G'Sell Florence, Zolynski Célia *et al*., « Enfants et écrans. À la recherche du temps perdu », rapport remis au Président de la République, avril 2024.

sur l'hyperconnexion des enfants et les stratégies développées pour capter l'attention, les contrôler et les monétiser. Plusieurs dangers pour les enfants sont énumérés comme le déficit de sommeil, la sédentarité, les problèmes de vues ou encore l'altération socio-émotionnelle et au développement du langage. Pour les adolescents, l'utilisation des réseaux sociaux augmente les risques de dépression ou d'anxiété. Il est important de rappeler qu'Instagram a été conçu comme une application de comparaison sociale.

18. Civilisation du poisson rouge. Au sujet de la captation de l'attention, Bruno Patino - auteur de l'ouvrage « La civilisation du poisson rouge » -, étudie l'économie de l'attention par les plateformes. Il compare l'attention du poisson rouge qui est de 8 secondes à celle de la génération des *Millennials* ayant grandi avec les écrans. Il détermine la capacité d'attention de cette génération à 9 secondes, soit seulement une seule de plus qu'un poisson rouge. Pour une société comme Google, ces secondes constituent un défi pour attirer l'attention de l'internaute grâce à des alertes incessantes et des messages instantanés. Ainsi, « Tel le poisson, nous pensons découvrir un univers à chaque moment, sans nous rendre compte de l'infernale répétition dans laquelle nous enferment les interfaces numériques auxquelles nous avons confié notre ressource la plus précieuse : notre temps.[76] ». Grâce à la collecte et l'utilisation des données des internautes, les GAFAM disposent d'informations essentielles pour attirer et garder l'attention sur leurs plateformes. Aujourd'hui, leur économie repose en grande partie sur la monétisation de notre temps de cerveau disponible[77].

19. Inconscience des utilisateurs. Les utilisateurs sont souvent inconscients de la manipulation dont ils font l'objet. À titre d'illustration, l'application Pokémon Go lancée durant l'été 2016 était loin d'être uniquement un divertissement altruiste pour les utilisateurs. En réalité, cette application - développée par Niantic (ex-Google), The Pokémon Compagny - caractérisait l'accomplissement du capitalisme de surveillance avec « un laboratoire vivant de la modification comportementale qui conjuguait avec aisance échelle, gamme et action[78] ». D'une part, l'application récoltait une grande quantité de données à caractère personnel des utilisateurs sur leurs téléphones. D'autre part, les utilisateurs n'étaient pas informés qu'ils

[76] Patino Bruno, *La civilisation du poisson rouge. Petit traité sur le marché de l'attention*, éd. Grasset, 2020, p. 15.

[77] Peugeot Valérie, « Données personnelles : sortir des injonctions contradictoires », VECAM (Citoyenneté dans la société numérique), 2014, disponible en ligne.

[78] Zuboff Shoshana, *op. cit*.

étaient simplement manipulés afin de se retrouver à endroits ne relevant en rien du hasard. En effet, les joueurs sont envoyés capturer des Pokemons à proximité d'établissements comme Starbucks ou McDonald's[79]. Plusieurs sociétés marchandes avaient payé pour avoir une augmentation de leurs clientèles. Pour autant, les utilisateurs sont souvent inconscients de la surveillance dont ils font ou sont l'objet.

20. Le capitalisme de surveillance. La notion de capitalisme de surveillance a été introduite en 2014 avec les éditeurs de la *Monthly Review* et popularisée par la sociologue américaine Shoshana Zuboff, professeure émérite à Harvard[80]. Le capitalisme de surveillance serait une nouvelle forme de capitalisme fondée sur les données : l'expérience humaine est traduite en données comportementales afin de produire des prédictions qui seront ensuite revendues sur le marché des comportements futurs[81]. Il s'agit de connaître l'ensemble des habitudes des consommateurs afin de les orienter vers des produits à acheter. La problématique du capitalisme de surveillance est qu'elle est invisible : il paraît plus difficile d'y échapper puisqu'elle n'est pas apparente[82]. Des services comme Gmail analysent le contenu des mails « d'une façon qui aurait conduit n'importe quel postier normal en prison[83] ». En effet, l'exploitation massive des données des utilisateurs par un nombre limité de sociétés est une atteinte invisible pour l'ensemble de notre vie privée.

---

[79] Lassègue Jean, *op. cit*.

[80] Bellamy Foster John, McChesney Robert, « Surveillance Capitalism », Monthly Review, 2014 ; Zuboff Soshana, *The Age of Surveillance Capitalism : The Fight for a Human Future at the New Frontier of Power*, éd. Profile Books, 2018.

[81] Cousin Olivier, « Le capitalisme de la surveillance », RPPI, n°1, juillet 2021, p. 11.

[82] Zuboff Shoshana, « Un capitalisme de surveillance. Votre brosse à dent vous espionne », sur Le Monde diplomatique, 2019 : « La politique d'accumulation des données rendant la surveillance plus performante était d'autant plus efficiente qu'elle était incolore, indolore, indéchiffrable. C'est le principe du miroir sans tain. Les utilisateurs se voient sans penser qu'ils sont vus, ils ont l'impression d'avoir la maîtrise de ce qui s'affiche sur l'écran, or ce qui est affiché est absorbé et exploité à leur insu. Chaque fois qu'un usager prenait conscience de la violation de sa vie privée, de l'accaparement de ses données et qu'il manifestait son désir de sortir de l'engrenage, on lui opposait une fin de non-recevoir, et ce, dès le début des plateformes numériques. Pas d'utilisation sans exploitation des data. La surveillance va de pair avec la logique de l'accumulation. Cette accumulation des données est comparable à l'accumulation du capital dans la théorie marxiste. ».

[83] Wylie Christopher, *op. cit*.

L'un des responsables de Google, Douglas Edwards déclarait en 2001 que « les gens vont générer d'énormes quantités de données […]. Tout ce que vous aurez entendu, vu ou éprouvé deviendra consultable. Votre vie entière deviendra consultable[84]. ». Quelques années plus tard, Viton Cerf, l'un des pères de l'Internet - qui travaille aujourd'hui chez Google -, déclarait que la vie privée est devenue une anomalie[85]. Ainsi, les entreprises du numérique ne se contentent plus de seulement collecter les données afin d'améliorer les services, il s'agit désormais de lire dans la pensée des individus afin de les manipuler et de servir leurs intérêts. Ils accumulent un nombre de données considérable et cela en partie par les gestes des consommateurs. L'essor des objets connectés permet à ces plateformes de cumuler toujours plus de données de consommation sur leurs utilisateurs et par conséquent, de perpétuer leur capitalisme de surveillance.

21. La « poignée de main invisible ». Pendant longtemps, les GAFAM ont écarté les règles de protection des données à caractère personnel sur le fondement de la sécurité afin de récolter les données de l'ensemble de la planète. Un véritable scandale de surveillance de masse par les autorités de surveillance avait été révélé par le lanceur d'alerte Edward Snowden en 2013. Durant plusieurs années, le programme « PRISM » de la FBI et de la NSA a permis de surveiller les internautes de la planète entière grâce à la collaboration des acteurs du numérique tels que Google, Microsoft, Facebook ou encore Apple[86]. Le programme permettait d'avoir accès aux *e-mails* des individus, à leurs photos, vidéos, pièces jointes, etc. pour un coût pratiquement nul pour le gouvernement[87]. Il s'agissait d'une « poignée de main invisible », c'est-à-dire d'un

---

[84] Douglas Edwards, *I'm Feeling Lucky : The Confessions of Google Employee Number*, éd. Allen Lane, 2011.

[85] Marin Jérôme, « La vie privée ? "Peut-être une anomalie", selon un responsable de Google », article Lemonde, 22 novembre 2013, disponible en ligne : https://www.lemonde.fr/pixels/article/2013/11/22/la-vie-privee-peut-etre-une-anomalie-selon-un-responsable-de-google_6002947_4408996.html.

[86] Lachapelle Amélie, « Le lancement d'alerte (whistleblowing) à l'ère du règlement général sur la protection des données », *in* De Terwangne Cécile, Rosier Karen (dir.), *Le règlement général sur la protection des données*, éd. Larcier, 2018, p. 797.

[87] Harcourt Bernard et Renaut Sophie, *La société d'exposition*, éd. Seuil, 2020, p. 17. « Et, bien que la NSA ait nié avoir un accès immédiat à ces données, les documents de la NSA divulgués par Edward Snowden établissent que l'agence revendique "la collecte directement auprès des serveurs" des principaux fournisseurs des États-Unis ». […] Le Guardian a expliqué, sur la base d'un document de la NSA daté d'avril 2013 : « Le programme Prism permet à la NSA, la plus grande organisation de surveillance du monde, d'obtenir des communications ciblées sans avoir à en faire la demande aux fournisseurs de services et sans avoir à obtenir d'ordonnance judiciaire. Grâce à ce programme, la NSA est en mesure d'accéder directement aux serveurs des entreprises participantes et d'obtenir des communications stockées, ainsi que d'effectuer des collectes en temps réel sur des utilisateurs ciblés. ».

« laisser faire » pratiqué par les autorités publiques américaines à l'égard des géants du numérique en l'échange de l'accès aux données collectées par ces entreprises[88]. Les pratiques de ces acteurs constituent un risque pour les libertés individuelles et particulièrement, pour le droit au respect de la vie privée.

22. Transferts des données aux États-Unis : les arrêts « Schrems ». Quelques années plus tard, le citoyen autrichien Maximillian Schrems a remis en question l'accord entre les États-Unis et l'Union européenne permettant certains transferts de données. En effet, les données peuvent être transférées auprès d'un pays tiers lorsque le pays en question assure un niveau de protection adéquat à ces données. La Commission européenne avait acté ce niveau de protection à l'égard des États-Unis dans une décision « Safe Harbour ». Monsieur Schrems va considérer qu'à la suite des révélations de l'affaire Snowden, les États-Unis n'offrent plus la protection suffisante contre la surveillance, par des autorités publiques, des données transférées[89]. Le 6 octobre 2015, la Cour de Justice de l'Union européenne annule la décision 2000/520 de la Commission européenne dite « Safe Harbour »[90]. La liberté des transferts de données entre l'Union européenne et les États-Unis était privée de base juridique. Rapidement, en février 2016, un nouveau « bouclier de protection des données » est conclu : le « Privacy Shield ». Le nouvel accord repose sur un mécanisme d'auto-certification des organisations américaines qui collectent les données afin de maintenir les accords commerciaux[91]. Le 16 juillet 2020, la Cour de Justice de l'Union européenne invalide à nouveau cet accord, rendant l'arrêt « Schrems II », en soulignant toutefois la validité des clauses contractuelles types de la Commission européenne[92]. Plus récemment, le 10 juillet 2023, la Commission européenne a adopté le « Data Privacy Framework » faisant suite à l'annulation du « Privacy Shield ». Toutefois, l'association

[88] Iliopoulou-Penot Anastasia, « La Constitution numérique européenne », RFDA, 2023, 945.

[89] Berlin Dominique, « Les retombées inattendues de l'affaire Snowden », La Semaine Juridique, n° 42, octobre 2015, 1107.

[90] Cour de Justice de l'Union européenne, aff. C-362/14, Schrems c/ Data Protection Comissionner, 6 octobre 2015 ; Castets-Renard Céline, « Invalidation du Safe Harbor par la CJUE : tempête sur la protection des données personnelles aux États-Unis », D., 2016, 88 ; Martial-Braz Nathalie, « Fumée blanche sur le front des transferts des données, really ? », CCE, n° 10, octobre 2023, 9.

[91] Crichton Cécile, « Transfert de données vers les USA », Dalloz Actualité, juillet 2020 ; Castets-Renard Céline, « Adoption du Privacy Shield : des raisons de douter de la solidité de cet accord », Dalloz IP/IT, 2016, 444.

[92] Cour de Justice de l'Union européenne, aff. C-311/18, DPC c. Facebook Ireland Ltd et M. Schrems, 16 juill. 2020 ; Bertrand Brunessen, « Les enjeux de la surveillance numérique », RTD eur., 2021, 175.

NOYB de Maximilian Schrems a déjà indiqué vouloir contester cet accord[93]. Les transferts de données constituent de véritables enjeux de souveraineté pour les États et les conséquences peuvent être lourdes d'un point de vue démocratique lorsqu'il s'agit de collecter des données dans un but de manipulation. En effet, le ciblage comportemental et la manipulation ont constitué ces dernières années des outils privilégiés de perturbation des processus électoraux et de déstabilisation démocratique. Les personnes peuvent être manipulées et influencées afin que leurs préférences servent des intérêts extérieurs[94].

23. Risques démocratiques : le scandale Cambridge Analytica. Le 17 mars 2018, le New York Times et l'Observer de Londres ont révélé qu'une société de conseil en stratégie basée à Londres, « Cambrige Analytica », avait exploité les données à caractère personnel de plus de 50 millions d'utilisateurs de Facebook, évidemment sans leur consentement, passant à 87 millions après réévaluation[95]. Pour ce faire, la société avait développé un test de personnalité - d'apparence anodin -, moyennant rémunération. Le test avait été créé par Aleksandr Kogan, psychologue de l'université de Cambridge, et lui avait permis d'accéder aux données à caractère personnel de deux cent soixante-dix mille membres de Facebook[96]. Une fois le questionnaire accepté, la société aspirait toutes les données à caractère personnel du profil de l'utilisateur mais également les profils de leurs amis. Le lanceur d'alerte de ce scandale, Christopher Wylie, expliquait que l'application permettait de collecter « le profil complet de dizaines de milliers d'utilisateurs - leur nom, leur genre, leur âge, leur ville, leurs mises à jour de statut, leurs *likes*, leurs "amis" - *tout,* en fait[97]. ». Les données étaient ensuite exploitées par la société, et utilisées pour transmettre des publications ciblées aux électeurs américains visant « leurs démons

---

[93] Schwartz Julie, « RGPD - Le Data Privacy Framework, entre réjouissances et critiques déjà présentes », Cahiers de droit de l'entreprise, n° 5, 25, 2023 ; Naftalski Fabrice, « Le nouveau cadre de protection des données Union européenne-États-Unis, portée et limites », Dalloz IP/IT, 2023, 600.

[94] Vergnolle Suzanne, *L'effectivité de la protection des personnes par le droit des données à caractère personnel*, éd. Larcier, 2022, introduction

[95] Manokha Ivan, « Le scandale Cambridge Analytica contextualisé », Cultures Conflits, n° 109, éd. L'Harmattan, 2018.

[96] Canonne Justine, « Cambridge Analytica : le rôle des psys dans le scandale », Sciences Humaines, n° 29, 2018.

[97] Wylie Christopher, *Mindfuck. Le complot Cambridge Analytica pour s'emparer de nos cerveaux,* éd. Bernard Grasset, 2020, p. 195 : « En utilisant l'application de Kogan, nous avons obtenu non seulement un jeu de données d'entraînement qui nous permit de créer un algorithme vraiment puissant - parce que les données étaient riches, denses, signifiantes -, mais aussi, en bonus, des centaines de profils supplémentaires d' "amis" Facebook, le tout pour un ou deux dollars par installation de l'appli. […] La réponse d'une seule personne entraînait en moyenne l'enregistrement de trois cents autres personnes. ».

intérieurs[98] ». Pire encore, la société avait développé sur Facebook de fausses pages qui ressemblaient à de vrais forums, de vrais groupes ou de vraies sources d'information. L'algorithme de recommandation dirigeait alors les utilisateurs vers ces groupes, selon leurs *likes* précédents et similaires. Dans cette histoire, même si les utilisateurs avaient sûrement inconsciemment « accepté » l'analyse de leurs profils, il est certain que leurs amis n'y avaient pas consenti[99]. Pour le lanceur d'alerte, le scandale de Cambridge Analytica démontre simplement que nos identités et comportements sont devenus des marchandises dans une économie de la donnée, grâce à des algorithmes conçus en secret qui influencent les esprits d'une manière encore inimaginable il y a peu[100]. En réalité, l'affaire Cambridge n'est qu'un exemple modeste des pratiques effectuées en matière de collecte de données et de violation de vie privée.

24. Risques pour l'environnement. Pour finir - et d'une manière non exhaustive -, un autre risque invisible existe et concerne l'ensemble des citoyens du monde : les atteintes des plateformes pour l'environnement. Pendant longtemps, le numérique a été associé à une image de légèreté, avec la dématérialisation ou encore le stockage « dans les nuages » pour le *cloud*[101]. Il n'en est rien, le numérique nécessite de nombreux équipements physiques, à l'instar des câbles sous-marins pour la circulation des données ou les infrastructures pour le stockage des données[102] ; l'immatérialité apparente du numérique dissimule une empreinte écologique très lourde[103]. Les centres de stockage des données nécessitent énormément d'eau afin de les refroidir. À titre d'illustration, Google révélait avoir utilisé 28 milliards de litres d'eau dans l'année dont les deux tiers pour refroidir ses centres de données[104].

---

[98] Cadwalladr Carole, Graham-Harrison Emma, « Revealed: 50 million Facebook Profiles Harvested for Cambridge Analytica in Major Mata Breach », The Observer, 17 mars 2018.

[99] Netter Emmanuel, *Regards sur le nouveau droit des données personnelles*, éd. CEPIRSCA, 2019, p. 9.

[100] Wylie Christopher, *op. cit*.

[101] Breteau Lise, « Numérique et environnement : émergence d'un sujet majeur », CCE, n° 12, décembre, 2023, étude 24.

[102] Hellio Hugues, « Les données numériques, nouvel objet et enjeux de souveraineté », *in* Nevejans Nathalie (dir.), *Données et technologies numériques*, éd. mare et martin, 2021, p. 170.

[103] Lequette Suzanne, *Droit du numérique*, éd. LGDJ, 2024, p. 23 ; Comité économique social et environnemental (CESE), « Impacts de l'intelligence artificielle : risques et opportunités pour l'environnement », Avis, 24 septembre 2024.

[104] Google, « Environnemental Report », 2023, disponible en ligne.

Par ailleurs, les technologies numériques consomment également énormément d'énergie : les technologies digitales mobilisent environ 10% de l'électricité produite et rejetteraient près de 4% des émissions globales de CO2, soit presque le double que les quantités d'émissions du secteur aérien mondial[105]. D'une manière regrettable, les émissions augmentent de façon exponentielle avec le développement de l'intelligence artificielle. Dans son dernier rapport environnemental 2023 publié en juin 2024, Google révélait une augmentation de plus de 48% de ses émissions depuis 2019 et près de 13% pour l'année 2023. En effet, l'intelligence artificielle consomme davantage d'énergie que les technologies précédentes : une requête sur un assistant d'intelligence artificielle comme ChatGPT mobilise dix fois plus d'énergie que sur un moteur de recherche traditionnel[106]. Ainsi, « pour envoyer un simple like, nous déployons ce qui sera bientôt la plus vaste infrastructure jamais édifiée par l'homme[107] ».

Au regard de l'ensemble des risques évoqués pour la vie privée des citoyens et l'environnement, il paraît nécessaire de rappeler que les entreprises du numérique sont avant tout des sociétés privées ayant pour unique objectif l'augmentation de leurs bénéfices. Le dessein d'un espace de liberté est devenu un rêve : « l'utopie initiale est en train de mourir, tuée par les monstres auxquels elle a donné naissance[108] ». Ainsi, les États membres ainsi que l'Union européenne s'engagent à construire de concert un cadre normatif afin d'encadrer et réguler les pratiques des géants du numérique.

---

[105] Hugues Ferreboeuf pour le Think Tank The Shift Project, « Pour une sobriété numérique », 2018, disponible en ligne.

[106] Martial-Braz Nathalie, « L'IA, mère de tous les maux environnementaux ! », CCE, n°9, septembre 2024 : « Si la feuille de route semble bien complexe, l'objectif - lui - paraît clair. Il s'agit de déterminer comment faire de l'IA une technologie moins polluante dont on ne craint pas que le développement, largement porteur de progrès, se fasse au détriment complet de notre planète. Il est impératif que cet enjeu soit pris davantage en compte à l'heure où l'on pèse les enjeux de cette technologie… et il est peut-être utile, ici comme ailleurs, d'éduquer à une certaine sobriété des usages. ».

[107] Pitron Guillaume, *L'enfer numérique : Voyage au bout d'un Like*, éd. Les Liens qui Libèrent, 2021, p. 17.

[108] Patino Bruno, *op. cit.*, p. 48 : « Deux forces ignorées par les libertaires se sont déployées en l'absence d'entrave : l'emportement collectif né des passions individuelles et le pouvoir économique né de l'accumulation. Nos addictions ne sont que le résultat du lien établi entre l'un et l'autre, et de la superstructure économique qui les fait se nourrir l'un de l'autre, se renforcer mutuellement au détriment de notre liberté. ».

II. La construction d'un cadre normatif

25. Notion d'idéalisme. Les États membres et l'Union européenne souhaitent encadrer les pratiques des géants du numérique afin de développer l'innovation en Europe et protéger la vie privée des citoyens : l'ambition est idéaliste et la construction est en cours. L'idéalisme renvoie à une attitude qui consiste à fonder son action ou sa conduite sur un idéal, c'est-à-dire un but élevé que l'on se propose d'atteindre. Le but ultime de la politique et du droit serait l'accomplissement d'une société parfaite, observant un respect total de la liberté humaine[109]. Dans la pratique du droit, les manifestations de l'idéalisme juridique revêtent plusieurs formes. Il peut s'agir de l'imprégnation par le droit de certains aspects ou notions du caractère idéal dans ses définitions, ses concepts ou ses règles. Il peut également s'agir du juge qui se réfère à une notion d'ordre idéal afin de renforcer son argumentation, tout en restant extérieur au droit positif. Enfin, il peut s'agir de la doctrine qui analyse une notion juridique au regard d'une théorie philosophique idéaliste[110]. Ainsi, par une interprétation théologique et fondationnelle, la règle de droit est envisagée selon un possible décalage entre l'idéal et ce que le législateur a tenté de réaliser[111].

Depuis quelques années, l'Union européenne développe une stratégie du numérique afin d'améliorer la société ou l'homme, en protégeant les individus contre les dérives des acteurs du numérique (A). En réalité, le fait d'avoir laissé perpétuer des pratiques contestables pendant un certain temps rend complexe l'élaboration d'une politique concrète. La stratégie idéaliste s'avère bousculée par des obstacles pratiques et des intérêts divergents, délibérément intensifiés par les géants du numérique (B).

A) L'idéalisme des objectifs de l'Union européenne

26. Enjeux de souveraineté. L'exploitation des données soulève des questions juridiques fondamentales : la protection des données personnelles, la souveraineté numérique des États ou encore la régulation des flux transnationaux de données. Afin d'encadrer les géants du

[109] Arnaud André-Jean, *Dictionnaire encyclopédique de théorie et de sociologie du droit*, éd. LGDJ, 2018, p. 280, sens 2).

[110] Oppetit Bruno, *Philosophie du droit*, éd. Dalloz, 2022, p. 110 ; Mongoin David, *Philosophie du droit*, éd. Dalloz, 2022, p. 312 sur l'opposition avec le réalisme.

[111] Sève René, *Philosophie et théorie du droit*, éd. Dalloz, 2016, p. 260.

numérique, les États membres partagent un idéal commun : celui de pouvoir protéger leurs citoyens contre les dérives des acteurs du numérique tout en développant l'innovation par l'exploitation des données. De fait, les États membres cherchent à maintenir ou retrouver une souveraineté. La souveraineté renvoie à l'indépendance des États membres, leur capacité à garder « la maîtrise de ses compétences les plus fondamentales et à appliquer les valeurs qui fondent sa raison d'être et son identité[112] ». La souveraineté numérique devient le prolongement de la notion de souveraineté dans l'espace numérique[113]. Pour les États membres, il s'agit d'établir leur capacité à garder ou rétablir leur souveraineté sur les outils numériques pour retrouver la maîtrise de nos réseaux et de nos données[114].

En effet, les États-Unis sont en situation d'une intense domination dans le domaine du numérique, pour la couche dite matérielle avec les infrastructures ou encore la couche logique avec les systèmes d'exploitation[115]. La couche logique est principalement conçue et structurée par des entreprises privées, ayant la propriété de la technologie[116]. L'Union européenne souhaite équilibrer ce *leadership* pratiqué par les États-Unis en encadrant les données des citoyens européens et en développant le potentiel des données à caractère non personnel. Pour ce faire,

---

[112] Bertrand Brunessen « La souveraineté numérique : quels enjeux politico-juridiques ? », *in* Bertrand Brunessen et Le floch Guillaume (dir.), *La souveraineté numérique*, éd. Bruylant, 2024, p. 1 ; Anne-Thida Norodom, « Être ou ne pas être souverain en droit, à l'ère numérique », *in* Castets-Renard Céline (dir.), *Enjeux internationaux des activités numériques : Entre logique territoriale des États et puissance des acteurs privés*, éd. Larcier, 2020, pp. 21-42 ; Byk Christian « La souveraineté numérique à l'heure de la gouvernance mondiale », Dalloz IP/IT, 2020, 337 ; Beauchesne Bénédicte « La dépendance européenne et nationale face aux nouveaux acteurs du numérique », Dalloz IP/IT, 2021, 125 ; Martial-Braz Nathalie, « Souveraineté numérique en danger ! », CCE, n°5, mai 2024.

[113] Türk Pauline, « L'exercice des fonctions de l'État à l'ère numérique » *in* Bertrand Brunessen et Le floch Guillaume (dir.), *La souveraineté numérique*, éd. Bruylant, 2024, p. 67 .

[114] Longuet Gérard, « Le devoir de souveraineté numérique », Assemblée Nationale, Rapport n° 7, Tome I, déposé le 1er octobre 2019.

[115] Hellio Hugues, « Les données numériques, nouvel objet et enjeux de souveraineté, *in* Nathalie Nevejeans (dir.), *Données et technologies numériques*, p. 170 : « Indéniablement, les États-Unis d'Amérique sont aujourd'hui en situation d'extrême leadership dans le domaine du numérique. Quelle que soit la couche des réseaux informatiques considérée, ils y exercent une hyper domination qui ne laisse aucun doute sur l'effectivité de leur souveraineté numérique. […] Pour la couche matérielle : cela vaut pour les câbles sous-marins de circulation des données. Les principaux sont reliés aux côtes atlantiques et pacifiques des États-Unis qui en ont ainsi un contrôle immédiat voire un pouvoir de censure. Cela vaut autant pour le stockage des données au sein de centres de données dont la majorité en nombre et en capacité est implantée sur le territoire états-unien. ».

[116] Chaigneau Aurore, « Propriété et souveraineté de l'internet : la maîtrise d'une infrastructure », *in* Netter Emmanuel et Chaigneau Aurore (dir.), *Les biens numériques*, éd. CEPRISCA, 2015, p. 25 : « Si les instances permettent de faire dialoguer tous les intérêts, la technologie n'appartient qu'à certains. ».

les États membres et principalement l'Union européenne construisent depuis plusieurs décennies un cadre normatif afin de faire face aux pratiques des acteurs du numérique : la construction désignant l'action d'élaborer un système politique ou social et d'en assurer la réalisation[117]. La quête de souveraineté des États membres et de l'Union européenne s'effectue principalement par le droit[118]. Ainsi, les États membres et l'Union européenne n'ont cessé de rechercher un équilibre entre la protection des données à caractère non personnel et l'ouverture des données à caractère non personnel pour permettre le développement de l'innovation[119]. Il existerait une véritable recherche de « souveraineté des données » pour les États membres[120].

27. Protection de la vie privée. Au niveau national, la France a été pionnière en matière de protection des données à caractère personnel. L'entrée en vigueur de la Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés a pour genèse un scandale de regroupement des données des citoyens français. Dans une édition du 21 mars 1974, le Monde avait titré en première page « Safari ou la chasse aux Français »[121]. La publication de cet article provoquait une vive réaction et une prise de conscience des individus sur les pratiques de fichage. Il s'agissait d'un projet élaboré par l'Institut national de la Statistique et des Études économiques (INSEE) permettant la création d'un système automatisé pour les fichiers administratifs afin de créer un répertoire des individus, connu sous l'acronyme « SAFARI ». L'idée était de regrouper des informations sur chaque individu, présenté sous un numéro d'identification unique et l'article de presse va dénoncer le caractère liberticide du système automatisé. Grâce au développement de l'informatique, les données allaient pouvoir être interconnectées et croisées afin de présenter une source importante d'informations sur les individus. Ultérieurement à ces révélations, le projet est suspendu et la Loi Informatique et Libertés est adoptée le 6 janvier 1978.

---

[117] CNRTL, v° Construction.

[118] Norodom « Être ou ne pas être souverain en droit à l'ère numérique », *in* Castets-Renard Céline (dir.), *Enjeux internationaux des activités numériques*, éd. Larcier, 2020, p.21.

[119] Bellanger Pierre, « Les données personnelles : une question de souveraineté », Le Débat, 2015/1, n°183, Gallimard, 2015, pp. 14-25.

[120] Castets-Renard Céline, « Souveraineté étatique et plateformes numériques : vers une coopération au sein du DSA ? », *in* Bertrand Brunessen et Le floch Guillaume (dir.), *La souveraineté numérique*, éd. Bruylant, 2024, p. 49.

[121] Boucher Philippe, « SAFARI ou la chasse aux français », Le Monde, 21 mars 1974.

Dès 1995, le droit européen a pris le relais avec l'entrée en vigueur de la directive 95/46/CE du 24 octobre 1995[122]. La Charte des droits fondamentaux de l'Union européenne instituera le droit à la protection des données à caractère personnel en un droit fondamental avec la création de l'article 8[123]. Subséquemment, les techniques et les risques vont évoluer avec l'émergence d'Internet et les nouvelles plateformes. Les menaces ne vont plus provenir de l'administration mais de la part d'entreprises privées. Afin de s'adapter aux technologies émergentes et aux nouvelles pratiques, le droit à la protection des données à caractère personnel devait être renouvelé[124].

Après de nombreuses négociations entre les différents États membres et d'intenses campagnes de *lobbying* de la part des géants du numérique, le Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données est entré en vigueur en mai 2018 (RGPD)[125]. L'objectif de ce règlement étant de fixer un cadre harmonisé dans l'ensemble du territoire de l'Union européenne pour faire face aux défis des géants du

---

[122] 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.

[123] Charte des droits fondamentaux de l'Union européenne, 2000, 364/01, article 8 : « 1. Toute personne a droit à la protection des données à caractère personnel la concernant. 2. Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accorder aux données collectées la concernant et d'en obtenir la rectification. 3. Le respect de ces règles est soumis au contrôle d'une autorité indépendante. ».

[124] Poullet Yves, « Avant-propos : le RGPD - une volonté de bien faire : certes ! ... mais appropriée ? », *in* De Terwangne Cécile, Rosier Karen (dir.), *Le règlement général sur la protection des données (RGPD/GDPR), Analyse appronfondie*, éd. Larcier, 2018, p. 10 : « À l'Internet encore balbutiant de 1995, on opposera bien volontiers l'existence désormais d'une toile globale et ubiquitaire, mêlant l'infiniment grand des capacités de nos ordinateurs (le Big Data) et de nos réseaux et l'infiniment petit (puces logées dans nos poches, dans nos lunettes, dans les objets voire dans nos cerveaux). C'est l'Internet des objets, les manipulations génétiques, fruits des NBIC, le cloud computing, l'intelligence artificielle qui déjà fait rêver les transhumanistes voire les post-humanistes et qui, de plus en plus, anime nos robots. Le texte du RGPD entend prendre en compte ces applications nouvelles à travers des précisions à propos des identifiants en ligne et des données de localisation (citées parmi les données à caractère personnel), des dispositions sur le profilage né de l'intelligence artificielle ou encore en évoquant, dans ses considérants, l'application à telle ou telle technologie. Il est certain que l'irruption de ces technologies modifie de manière sensible les modes de collecte, de traitement, de stockage et d'exploitation des données à caractère personnel. ».

[125] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).

numérique. La nature du règlement devrait permettre *a priori* d'établir un cadre harmonisé pour l'ensemble des États membres, au contraire de la directive[126]. La directive 95/46/CE du 24 octobre 1995 avait fait apparaître des divergences entre les États membres, dont les géants du numérique avaient profité pendant de longues années[127]. Le règlement est audacieux et conditionne le développement de l'économie de la donnée à la protection des droits fondamentaux, afin de « servir l'humanité »[128].

28. Libre circulation des données. Par ailleurs, la protection des données à caractère personnel conditionne la libre circulation des données : les données à caractère personnel doivent circuler librement d'un État à un autre, tout en respectant les droits fondamentaux des personnes. En effet, la libre circulation des données représente un enjeu économique majeur et dès les années 1980, la convention 108 avait instauré la libre circulation des données[129]. Il convient de prendre en compte la logique économique qui imprègne le droit de l'Union : la libre circulation des données est placée au même rang que la protection des données à caractère personnel. Il s'agit d'un objectif fondamental pour le développement du marché intérieur de l'Union européenne.

En parallèle, les données à caractère non personnel doivent également circuler librement afin de promouvoir l'innovation. Les données à caractère personnel sont incroyablement

---

[126] Norodom Anne-Thida, « Le RGPD, un standard européen de protection au regard du droit international », *in* Bensamoun Alexandra, Bertrand Brunessen et Anca AilincaiI Mihaela, Martial-Braz Nathalie (dir.), *Le règlement général sur la protection des données. Aspects matériels et institutionnels*, éd. Mare & Martin, 2020, pp. 83-127.

[127] Poullet Yves, « 50 ans de législations européennes de protection des données. Hier, aujourd'hui et demain », *in* Bévière-Boyer Bénédicte, Dibie Dorothée et Arlotti Clément (dir.), *Numérique, droit et société*, éd. Dalloz, 2022, p. 21 : « Sans doute, l'adaptation aux besoins de protection de notre vie privée et de nos données s'est-elle révélée rapidement insuffisante ou plutôt dépassée par les progrès technologiques. Sans doute, les disparités d'application de la directive avaient conduit la Commission à conclure à la nécessité d'un instrument ayant un effet direct sur l'ensemble du territoire de l'Union européenne. ».

[128] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), considérant 4 : « Le traitement des données à caractère personnel devrait être conçu pour servir l'humanité. ».

[129] Le Goffic Caroline, Pailler Ludovic et Grynbaum Luc, *Droit des activités numériques*, éd. Dalloz, 2023, p. 854 : « La circulation des données d'un État à un autre a été rapidement appréhendée comme un enjeu économique majeur. Dès les années 1980, les lignes directrices de l'OCDE puis la convention 108, la libre circulation des données d'un État à un autre est l'un des objectifs assignés au droit de la protection des données afin de favoriser le développement économique et social. ».

nombreuses, il peut s'agir des données issues de capteurs, des objets connectés ou encore des données industrielles. Les données à caractère non personnel apportent une valeur ajoutée significative aux services existants et de développer de nouveaux modèles d'affaires[130]. En effet, la circulation des données à caractère non personnel permet la création de nouveaux services et le renforcement de la compétitivité des entreprises européennes. L'Union européenne souhaite donc garantir la libre circulation des données à caractère non personnel en Europe. Pour ce faire, un règlement sur le libre flux des données à caractère non personnel est entré en vigueur en novembre 2018[131] et instaure un espace de libre circulation des données au sein de l'Union européenne.

29. Marché unique numérique. Le règlement sur le libre flux des données résulte d'une stratégie européenne proposée en 2015 : la stratégie pour un marché unique numérique. La communication de la Commission européenne définit le marché unique numérique comme « un espace dans lequel la libre circulation des biens, des personnes, des services et des capitaux est garantie. Un espace où les particuliers et les entreprises peuvent, quels que soient leur nationalité et leur lieu de résidence, accéder et se livrer à des activités en ligne dans un cadre garantissant une concurrence loyale et un niveau élevé de protection des consommateurs et des données à caractère personnel. ». Il s'agit de prendre le contrôle sur le marché mondial du numérique - dominé par les GAFAM - en accentuant l'ouverture et l'exploitation des données à caractère non personnel[132]. Pour cela, l'Union européenne doit résoudre le conflit entre l'ouverture des données dans une logique de marché intérieur et la protection des données à caractère personnel dans une logique de protection des citoyens européens.

30. Marché européen des données. Allant encore plus loin, la Commission européenne propose en 2020 « Une stratégie européenne pour les données ». Cette fois-ci, il s'agit de permettre à l'Union européenne de devenir un acteur de premier plan dans une société axée sur les données. La création d'un marché unique des données ouvre la libre circulation des données à caractère non personnel tout en renforçant la protection des données à caractère personnel. La

[130] Commission européenne, « Libre circulation des données à caractère non personnel », disponible en ligne.

[131] Règlement (UE) 2018/1807 établissant un cadre applicable au libre flux des données à caractère non personnel dans l'Union européenne.

[132] Barreau Catherine, « Le marché unique numérique et la régulation des données personnelles », Réalités industrielles, août 2016 ; Castets-Renard Céline, Ndior Valère et Rass-Masson Lukas, « Le marché unique numérique : quelles réalités matérielles et conceptuelles ? », D., 2019, 956.

Commission rappelle que « dans une société où les individus génèrent des volumes toujours plus importants de données, la façon dont les données sont collectées et utilisées doit placer les intérêts de l'individu en première place, conformément aux valeurs, aux droits fondamentaux et aux règles de l'Union européenne » tout en rappelant que « dans le même temps, le volume croissant de données des secteurs privé et public à caractère non personnel en Europe, combiné à l'évolution technologique pour le stockage et le traitement des données, constituera une source potentielle de croissance et d'innovation dont il convient de tirer parti ». La Commission souhaite la création d'un marché où les données à caractère personnel et les données à caractère non personnel provenant du monde entier soient en sécurité afin de stimuler la croissance et de créer de la valeur[133]. L'Union européenne envisage de faire de l'Europe un acteur de premier plan pour l'intelligence artificielle[134] dont les données sont la matière première[135]. De fait, l'accès à une quantité importante de données devient un préalable nécessaire au développement de l'intelligence artificielle en Europe.

La stratégie européenne n'est pas ou plus de créer un géant européen mais de mener un nouveau combat sur l'ouverture des données à caractère non personnel afin de développer l'intelligence artificielle[136]. L'idéal est désormais axé sur l'intelligence artificielle et la maîtrise des

[133] Commission européenne, « Une stratégie européenne pour les données », Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions, COM(2020) 66 final, février 2020, p. 5.

[134] Deffains Bruno et Coudray Chloé, « La construction d'une politique européenne du numérique », *in* Bertrand Brunessen, *La politique européenne du numérique*, éd. Bruylant, 2023, p. 50 : « Outre leur potentiel pour la croissance économique et pour relever les défis sociétaux, les données constituent la base du développement des applications d'intelligence artificielle, qui nécessitent le traitement de vastes quantités de données de haute qualité. ».

[135] Bertrand Brunessen, « La gouvernance des données dans la régulation européenne de l'intelligence artificielle », RTD eur., 2022, n° 315, « Les données sont au cœur de l'intelligence artificielle. Ce sont les données qui vont permettre de penser, construire, définir, façonner, faire évoluer et tester la fiabilité de l'intelligence artificielle. Si la gouvernance des données n'épuise pas les enjeux de la régulation de l'intelligence artificielle, elle contribue, de façon fondamentale, à la définir. Les caractéristiques d'un système autonome peuvent ainsi, par avatisme, largement être comprises à la lumière des données utilisées pour son élaboration, qu'il s'agisse de données d'entraînement, d'entrée, de validation ou de test. » ; La Commission européenne le rappelle dans son Livre blanc « Intelligence artificielle. Une approche européenne axée sur l'excellence de la confiance, COM(2020) 65 final, 19 février 2020, p. 9 « sans données, il est impossible de développer des applications d'intelligence artificielle et d'autres applications numériques. ».

[136] Latil Arnaud, *Le droit du numérique*. *Une approche par les risques*, éd. Dalloz, 2023, p. 26.

données[137]. Dès lors, plusieurs règlements sont entrés en vigueur afin de réguler le marché des données et de poursuivre le mouvement d'ouverture des données. L'Union européenne a élevé le statut du numérique au rang des priorités stratégiques définies par les institutions européennes[138]. D'une manière louable la construction du cadre normatif se poursuit au prisme des valeurs européennes, c'est-à-dire le renforcement de la protection des individus sans entraver le développement technologique[139]. À ce titre, une Déclaration européenne sur les droits et principes numériques pour la décennie a été proclamée par l'Union européenne le 15 décembre 2022. La déclaration rappelle que « la technologie doit servir et bénéficier à tous les citoyens de l'Union européenne et leur permettre de poursuivre leurs aspirations, en toute sécurité et dans le respect des droits fondamentaux[140] ».

Néanmoins, l'idéalisme est opposé au réalisme. Le réalisme désigne la capacité à prendre en compte les données d'une situation avant de prendre une décision ou d'agir. En réalité, les États membres sont confrontés à de nombreuses difficultés résultant de l'opacité et l'inintelligibilité des pratiques des géants du numérique. Par ailleurs, les acteurs du numérique agissent de manière subreptice afin de garder la maîtrise sur les données, matière première de leur modèle d'affaires.

---

[137] Bertrand Brunessen, « L'émergence d'une politique européenne "spontanée" du numérique », *in* Bertrand Brunessen, *La politique européenne du numérique*, éd. Bruylant, 2023, p. 29 : « Au lieu de mener le combat perdu des données personnelles, les institutions européennes ambitionnent de placer le débat sur le terrain des données non personnelles et ainsi de définir une voie proprement européenne qui se distinguent des visions chinoises et américaines : penser une protection des individus, de leurs droits, sans entraver excessivement le développement industriel et technologique. ».

[138] Marti Gaëlle, « Les instruments normatifs de la politique du numérique », *in* Bertrand Brunessen, *La politique européenne du numérique*, éd. Bruylant, 2023, p. 236 : « L'intensification normative se donne à voir par l'accroissement quasi exponentiel des textes consacrés au numérique. Sur le plan quantitatif tout d'abord, on peut noter que les actes juridiques qui sont consacrés (en tout ou partie) au numérique sont passés d'une cinquantaine en moyenne par an avant les années 2000, à une centaine par an autour des années 2010 pour avoisiner les deux cents textes annuels en moyenne les dernières années. ».

[139] Castets-Renard Céline, « Enjeux géopolitiques et juridiques de l'intelligence artificielle : quelle stratégie pour l'Union européenne ? », *in* Castets-Renard Céline (dir.), *Enjeux internationaux des activités numériques : Entre logique territoriale des États et puissance des acteurs privés,* éd. Larcier, 2020, p. 78 : « L'Union européenne cherche donc à s'inscrire dans la compétition internationale naissante, mais aussi à encourager une forme de coopération tenant compte des risques de l'IA envers les droits fondamentaux et la sécurité des personnes. La Commission européenne est résolue à favoriser les avancées scientifiques, à préserver les atouts technologiques de l'Union et à faire en sorte que les nouvelles technologies soient au service de tous les Européens, c'est-à-dire qu'elles améliorent leur quotidien, tout en respectant leurs droits. ».

[140] Déclaration européenne sur les droits et principes numériques pour la décennie numérique, 2023/C 23/01, Chapitre I, « Placer l'humain au centre de la transformation numérique » .

B) Le pouvoir d'influence des acteurs du numérique

31. Instabilité de l'environnement. Les géants du numérique ont mis fin à l'utopie de liberté sur Internet. En privatisant les services et en captant les données des utilisateurs, les vœux des pionniers d'Internet se sont évaporés. La construction d'un cadre normatif est une opération complexe compte tenu de l'environnement numérique : un espace sans frontière gouverné par des flux mondiaux de données. Les enjeux et les effets extrapatrimoniaux sont remis en cause par cet environnement[141]. La notion de frontière, permettant de définir l'espace où un État peut exercer sa souveraineté, est largement remise en question par la circulation mondiale des données[142]. Par ailleurs, la technique et les technologies émergentes sont d'une vélocité sans précédent. Il convient alors d'encadrer cette « réalité nouvelle qui fait face à un changement multicentrique[143] ». L'environnement numérique complexifie l'opération d'encadrement des pratiques du numérique, longtemps régit par l'irresponsabilité des acteurs.

32. L'irresponsabilité des acteurs : une volonté idéaliste. Les premières législations étaient fondées sur une approche économique libérale afin de ne pas brider le développement des technologies du numérique[144]. À titre d'illustration, la directive 2000/31/CE du Parlement et du Conseil du 8 juin 2000 dite « Directive sur le commerce électronique » avait instauré un mécanisme d'irresponsabilité des fournisseurs de services numériques pour ne pas entraver leur développement[145]. Le régime d'exonération de responsabilité était instauré en fonction du type d'activité. Néanmoins, les enjeux du numérique ont considérablement évolué et les catégories

---

[141] Poullet Yves, « 20 ans de recherche au CRID », *in* Burkert Herbert, Lerouge Jean-François, Pichault François, Poulin Daniel, Poullet Yves, Vivant Michel (dir.), *Variations sur le droit de la société de l'information*, éd. Bruylant, 2002, p. 18 : « Le média Internet est global. Ce fait justifie que la question du droit applicable devient centrale. L'avènement d'Internet efface en effet les frontières traditionnelles et implique par là même la perte d'efficacité d'un certain nombre de législations nationales. ».

[142] Vivant Michel, « Internet et droit », p. 97 : « La spécificité première du phénomène, la plus évidente, est certainement que l'Internet ignore les frontières et même que les frontières sont une notion qui n'a plus de sens dans le cyberespace. Or cela est contradiction ouverte avec l'idée de souveraineté à l'instant évoquée puisque souveraineté renvoie à nation : frontières politiques contre réseaux sans frontières. Le défi est grand. Il est indiscutablement malaisé à relever. ».

[143] Gautrais Vincent, « La souveraineté numérique et dépendance des États », *in* Bertrand Brunessen et Le Floch Guillaume (dir.), *La souveraineté numérique,* éd. Bruylant, 2024, p. 109.

[144] Iliopoulou-Penot Anastasia, « La Constitution numérique européenne », RFDA, 2023, 945.

[145] Directive 2000/31/CE du Parlement 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 (« directive sur le commerce électronique »).

sont devenues trop restreintes à la réalité des pratiques. Les services fonctionnent pourtant *a priori* de façon identique à ceux d'un hébergeur, permettant à ces plateformes de bénéficier du régime de responsabilité associé. Le passage d'un web « consultatif » à un web « participatif » avec l'émergence des réseaux sociaux a bouleversé les usages : les réseaux sociaux sont restreints à un espace contributif gratuit puisque les sociétés se rémunèrent grâce à la publicité ciblée[146].

Au sujet de la politique d'utilisation des données, ils ont longtemps imposé leurs normes à travers leurs conditions générales d'utilisation[147]. En réalité, lorsqu'on laisse des pratiques se développer sans entrave pendant un certain temps, il devient complexe de les remettre en cause par la suite avec le droit. Depuis leur création, ils ont développé leur propre écosystème avec leurs propres règles. De par ce laisser faire, ils ont pu acquérir une hégémonie sur les données et la maîtrise de leur environnement et des technologies émergentes qu'ils élaborent.

33. L'opacité des pratiques. Nos comportements n'ont jamais été autant collectés et analysés, et ce en fonction d'un code informatique opaque et de critères absolument inintelligibles[148]. Par exemple, l'une des caractéristiques de l'intelligence artificielle réside dans son opacité : lorsque les systèmes évoluent grâce à l'apprentissage profond et non sur une programmation en amont, leur fonctionnement devient presque impossible à traduire ou

---

[146] Besse Thomas, « L'évanescente responsabilité pénale des fournisseurs de services intermédiaires dans le cadre de la mise en ligne de contenus illicites », Cahiers de la recherche sur les droits fondamentaux, Presses universitaires de Caen, 2023 ; Malka Richard, « La gratuité, c'est le vol », Le Débat, n° 188, 2016 ; Netter Emmanuel, « La publicité ciblée n'est pas "nécessaire" au contrat de réseau social. Le crépuscule d'un modèle d'affaires », RTD com., 2023, 359 : « Il suffit pour cela d'observer la manière dont ils interagissent avec le service : publications produites, commentées et "aimées" ; requêtes soumises au moteur de recherche... Les entreprises proposent ensuite aux annonceurs de relayer leurs messages commerciaux auprès d'un public soigneusement choisi pour sa réceptivité supposée au bien ou service proposé. L'efficacité est supposée maximale, même si la performance véritable du procédé est difficile à mesurer. Sur cette idée, on a bâti des empires. » ; Le Règlement (UE) 2022/2065 du 19 octobre 2022 du Parlement européen et du Conseil relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (règlement sur les services numériques) modernise le cadre à l'aune de l'émergence des réseaux sociaux.

[147] Anastasia Iliopoulou-Penot, *op. cit*.

[148] Rouvroy Antoinette et Berns Thomas, « Gouvernementalité algorithmique et perspectives d'émancipation. Le disparate comme condition d'individuation par la relation ? », Réseaux, n° 177, 2013 : « L'inoffensivité, la "passivité" du gouvernement algorithmique n'est alors qu'apparente : le gouvernement algorithmique "crée" une réalité au moins autant qu'il l'enregistre. Il suscite des "besoins" ou désirs de consommation, mais de la sorte il dépolitise les critères d'accès à certains lieux, biens ou services ; il dévalorise la politique (puisqu'il n'y aurait plus à décider, à trancher, dans des situations d'incertitude dès lors que celles-ci sont d'avance désamorcées) ; il dispense des institutions, du débat public ; il se substitue à la prévention (au profit de la seule préemption), etc. », pp. 163-196.

expliquer[149]. Les algorithmes vont « s'exprimer dans un espace qui leur est propre, et qui n'a pas fonction à être humainement compréhensible[150] ». Les géants du numérique sont pourtant soumis à une obligation de transparence de leurs outils. Néanmoins, il est probable que l'obligation de transparence ne permette pas de détecter les biais présents dans les algorithmes[151]. En tout état de cause, la transparence se heurte à la complexité des algorithmes[152]. Ils détiennent une supériorité sur leur propre code informatique, leur permettant d'échapper *a priori* à toute régulation[153].

34. Pouvoir normatif du code. Les mutations constantes des technologies perturbent les outils classiques de régulation et les fondamentaux immuables. En effet, la complexité de leurs pratiques rend difficile toute opération de normativité : lorsque la technique n'est pas intelligible, *de facto* la règle juridique ne peut l'être. En pratique, lorsque certaines pratiques des géants du numérique ne sont pas compréhensibles, l'autorégulation devient l'unique dénouement pour encadrer leurs pratiques avec leurs propres normes : « l'impression est celle d'une machine folle, dont les créateurs sont sommés de devenir les réparateurs[154] ».

Lawrence Lessig avait dans son célèbre article « Code is law » mis en exergue le fait que le code informatique détermine les conditions de protection de la vie privée puisque l'architecture de protection de la confidentialité dépend des choix de ceux qui élaborent le code[155]. Elle soulève que la technologie n'est pas neutre mais relève bien d'un choix politique[156]. De fait, les

---

[149] Bertrand Brunessen, « L'émergence d'une politique européenne du numérique », RTD eur., 2021, 129.

[150] Deltorn Jean-Marc, « Le droit des données personnelles face à l'opacité des algorithmes prédictifs : les limites du principe de transparence » *in* Netter Emmanuel (dir.), *Regards sur le nouveau droit des données personnelles*, éd. CEPRISCA, 2019, p. 153.

[151] Bertrand Brunessen et Sirinelli Jean, *op. cit*.

[152] Deltorn Jean-Marc, « Des données à la décision algorithmique : la notion juridique "d'explication" à l'épreuve des procédés d'apprentissage », *in* Nevejans Nathalie (dir.), *Données et technologies numériques*, éd. Mare et Martin, 2021, p. 83.

[153] Toledano Joëlle, *GAFA. Reprenons le pouvoir*, éd. Odile Jacob, 2020, p. 70 : « Dans ces gigantesques écosystèmes où les algorithmes gouvernent l'ordonnancement et les mises en relation, les règles sont inscrites dans des lignes de code informatique. […] Développés dans une logique d'efficacité économique à vocation d'emblée mondiale, ils s'embarrassent d'autant moins des lois applicables qu'elles peuvent être couteuses dans forcément leur apparaître pertinentes. ».

[154] Patino Bruno, *Tempête dans le bocal*, éd. Grasset, 2022, p. 16.

[155] Lawrence Lessig, « Code is Law : On Liberty in Cyberspace », Harvard Magazine, January-Februay, 2000.

[156] Teller Marina, « Vers l'acceptabilité sociale des algorithmes ou comment passer de l'"algocratie" à la démocratie algorithmique », Revue pratique de la prospective et de l'innovation n° 1, mai 2022, dossier 6.

géants du numérique étant motivés par des intérêts mercantiles, leurs algorithmes en sont pleinement imprégnés. L'ambition des géants du numérique serait de substituer la norme technologique à la norme juridique[157], c'est-à-dire de supplanter la norme juridique par le code informatique[158]. Le danger de cette substitution serait toutefois que les dispositifs technologiques remplissent les mêmes fonctions que les dispositifs juridiques, mais de manière plus rapide et plus efficace.

35. L'émergence d'une « algocratie ». Le pouvoir normatif du code informatique entraîne des problématiques d'accessibilité du code et par conséquent, du droit[159]. Le droit nécessite d'être compréhensible et accessible par tous et pour tous. En pratique, une asymétrie découle entre les programmateurs et les juristes : les programmateurs ont besoin des juristes pour élaborer leurs algorithmes mais l'inverse n'est pas vrai et les juristes n'ont pas d'accès direct au programme informatique[160]. L'avènement de l'« algocratie » caractériserait ce nouveau pouvoir d'internalisation des règles au sein du code informatique. Le « centre de gravité normatif » passerait par un processus d'auto-organisation du code des algorithmes[161]. Ainsi, les acteurs du numérique deviennent décisionnaires de l'application de la norme, dans un contexte extrêmement opaque. Autrement dit, l'effectivité des normes résulte des acteurs du numérique qui établissent les algorithmes[162].

---

[157] Teller Marina, *op. cit*. : « l'introduction de dispositifs algorithmes couplés à des systèmes d'intelligence artificielle précipite une forme de numérisation du droit, dont l'ambition plus profonde serait de substituer une norme technologique à une norme juridique. ».

[158] Groffe-Charrier Julie, « La loi est-elle dictée par le code ? », Dalloz IP/IT, 2020, 602.

[159] Teller Marina, « La deep law, ou le défi d'une "analyse numérique du droit" (Doit-on penser autrement le droit dans l'économie numérique ? », *in* Couret Alain (dir.), *Un juriste pluriel*, éd. Dalloz, 2020, p. 874.

[160] Prevost Jean-Baptiste, « La fabrique des données : à propos du codage numérique du droit et de ses limites », Gazette du Palais, 22 janvier 2019, n° 3, pp. 81-86 : « Mais la langue du code et la langue de la programmation (et donc le cœur des algorithmes) sont au contraire fondamentalement inaccessibles au commun des mortels, et les juristes n'ont donc aucun contrôle direct de la juste transcription de leur savoir dans les programmes que les ingénieurs élaborent. Le langage informatique, dont les fondements sont logico-mathématiques, se déploie comme un "langage" qui, à la différence de l'écriture, n'est pas transmissible en dehors de son milieu d'origine. C'est un "langage" que le concepteur anime de propriétés particulières et dont le fonctionnement engendre des effets très variables dans la structuration des données, des effets qu'il est difficile de reconduire clairement aux différents éléments du programme qui en sont la cause, ce qui a pour effet de restreindre la compréhension éventuellement critique de tel ou tel résultat. ».

[161] Gautrais Vincent, « La souveraineté numérique et dépendance des états aux technologiques » *in* Bertrand Brunessen et Le Floch Guillaume (dir.), *La souveraineté numérique*, éd. Bruylant, 2024, p. 110.

[162] Eltis Karen, « It's just the algorithm », *in* Bertrand Brunessen (dir.), *La politique européenne du numérique*, éd. Bruylant, 2023, p. 83 : « L'explication derrière ce phénomène [algocratie] prend source dans le fait qu'il est notoirement difficile pour une victime de détecter une attribution inappropriée faite à son

36. Pouvoir d'influence. En parallèle, grâce à l'opacité de leurs pratiques, les acteurs du numérique parviennent à influencer les normes[163]. Tout d'abord, ils prônent l'autorégulation afin de garder la maîtrise de leurs techniques et lorsque l'autorégulation est mise de côté, ils deviennent co-producteurs des normes[164]. Ils sont devenus des acteurs incontournables pour définir conjointement les normes avec les législateurs. D'une manière utopique, il existerait une relation de confiance entre le législateur et les géants du numérique[165] : les sociétés éclairent le législateur sur le développement des technologies émergentes afin d'élaborer des normes idoines. En réalité, il s'agit d'influer sur les normes dans leur propre intérêt, c'est-à-dire un intérêt lucratif et unilatéral[166]. Leurs intérêts auprès des instances européennes sont défendus par des pratiques de *lobbying*, dont les montants sont exorbitants[167]. Depuis quelques années, ils sont devenus le secteur investissant le plus d'argent à Bruxelles, tous secteurs d'activité confondus. À titre de comparaison, ils dépensent davantage que l'industrie pharmaceutique. De

égard par la "boite mystérieuse", opaque et insoluble, que constitue l'intelligence artificielle, d'autant qu'il est encore plus ardu de la constester. ».

163 Delmas-Marty Mireille, *La refondation des pouvoirs. Les forces imaginantes du droit (III)*, éd. Le Seuil, 2009, p. 144.

164 Raffray Romain, « Les multinationales et la création du droit », *in* Caire Anne-Blandine (dir.), *Les nouveaux pouvoirs. Approche pluraliste des foyers de création du droit*, éd. Bruylant, 2017, p. 75 : « La place des multinationales dans la création du droit a incontestablement changé en 30 ans. À l'époque, la création normative des multinationales s'insérait dans le cadre de la lex mercatoria. […] Les entreprises multinationales peuvent intervenir à tous les stades de la régulation publique au moyen de différents procédés de lobbying, de collaboration et de consultation. Du côté de la norme étatique, c'est donc la coproduction qui inquiète, les multinationales étant devenues si incontournables qu'elles sont en mesure d'influencer directement les choix législatifs. ».

165 Laurens Sylvain, « Au-delà du lobbying, réflexions sur l'appropriation privée du capital bureaucratique », Entreprises et histoire, 2021, pp. 32-44 : « Dans certaines configurations, ces approches ont amené une meilleure connaissance des systèmes politiques contemporains, notamment si l'on considère la littérature sur les institutions européennes. Ainsi, Arndt Wonka et Andreas Warntjen invitent à considérer les relations quotidiennes ou informelles qui se nouent autour des institutions de l'Union Européenne afin d'intégrer la manière dont "l'information technique" transmise par les entreprises influencerait ou non les "instruments de politique publique" : "l'information est le moyen de l'influence" résument-ils. ».

166 Bensamoun Alexandra, « Les mutations de la norme en droit d'auteur (réflexion sur les sources) », *in* Braz-Martial Nathalie, *Les mutations de la norme. Le renouvellement des sources du droit*, éd. Economica, 2000, p. 59 ; Malinvaud Philippe, « Lobbying et construction », RDI, 2012, p. 361.

167 Younan Sarah, « Européennes 2024 : quels sont les lobbies les plus puissants au Parlement européen ? », article Capital, disponible en ligne : « Des entreprises américaines représentées par un secteur en particulier depuis quelques années : la tech. En 2023, l'ensemble des sociétés de la tech américaine a dépensé 113 millions d'euros en activités de lobbying, toujours d'après les données recueillies par le site lobby facts. Avec 8 millions d'euros de budget annuel, Meta (Facebook, Instagram, Threads) est le groupe qui dépense le plus en lobbying à Bruxelles, suivi d'une partie des autres GAFAM. Apple alloue 7 millions d'euros au lobbying à Bruxelles, Google, 5,5 millions et Microsoft, 5 millions d'euros. ».

par leur influence, le droit devient négocié et cela impacte assurément la cohérence du cadre normatif.[168]. L'ensemble des modèles d'affaires des GAFAM repose sur les données[169]. Ainsi, les récentes réformes de l'Union européenne au sujet des données menacent leur modèle commercial. La construction d'un cadre normatif dominé par la technique et contrôlée par des entreprises privées s'avère être une opération périlleuse : « la construction entre le droit et la technique n'est pas nouvelle, mais les intelligences artificielles peuvent vite donner le tournis, dès lors qu'on évoque leur opacité et leur complexité[170] ».

37. Problématique générale. La présente thèse constitue une étude approfondie du cadre normatif des données dont la construction réside dans la recherche d'un équilibre idéaliste entre des intérêts et des objectifs divergents, voire antagonistes.

Ainsi, depuis plusieurs années, l'Union européenne a fondamentalisé la protection des données à caractère personnel. En parallèle, l'ouverture des données constitue un enjeu économique déterminant pour le marché intérieur. L'étude nécessite d'analyser la manière dont l'Union européenne assure la protection des données à caractère personnel et les exigences du marché intérieur. Pour autant, au regard des objectifs économiques louables, la protection des données à caractère personnel devient une aspiration impactée. Comment sera-t-il possible de concilier les principes idéaux tels que la vie privée et la protection des données à caractère personnel avec la réalité économique ? En effet, l'influence et la domination des géants du numérique bouleversent la construction d'un cadre normatif. L'environnement du numérique permet à ces acteurs d'avoir recours à l'autorégulation et d'influencer sur la construction des normes. Ils déploient leur influence auprès des instances européennes afin d'intégrer leurs intérêts dans les

---

168 Zolynski Célia, Bensamoun Alexandra, « La promotion du droit négocié en propriété intellectuelle : consécration d'une conception dialogique du droit », D., 2011, 1773.

169 Marty Frédéric, « Économie de la donnée. Écosystèmes numériques, algorithmes et intelligence artificielle. », *in* Jean-Michel Bruguière (dir.), *L'émergence d'un droit des données*, Dalloz, 2023, p. 25 : « Une plateforme peut détenir un avantage sur ses concurrents au travers des flux de données qu'elle peut capter, mais elle peut également par ce moyen même détenir une position de force vis-à-vis de ses partenaires et de ses utilisateurs. La plateforme qui parvient à centraliser les données et à les valoriser le plus efficacement est capable d'acquérir une position dominante écrasante et de devenir un partenaire incontournable pour les autres acteurs du marché. L'avantage concurrentiel se base alors sur la donnée et sur les capacités de traitement algorithmique de cette dernière. ».

170 Castets-Renard Céline, « Nouvelles technologies et droit européen : quel droit face à l'intelligence artificielle ? » , *in* Peyrou-Pistouley Sylvie (dir.), *Nouvelles technologies et droit européen : quel droit face à la disruption numérique ?*, éd. Mare et Martin, 2022, p. 13 ; De Gregorio Giovanni, « The normative power of artificial intelligence », Catolica Global School of Law Working Paper, n° 4/2023.

normes. Les géants du numérique bénéficient-ils de l'antagonisme des objectifs de l'Union européenne afin de promouvoir leurs intérêts et d'impacter délibérément la cohérence des normes ? Il conviendra alors de déterminer si le cumul de puissances de ces entreprises privées ne leur permet pas de contourner les lois au détriment de la protection des données à caractère personnel et de quelle manière le législateur assure la disponibilité des données en faveur des personnes concernées dans une logique alternative aux modèles d'affaires des entreprises du numérique.

38. Annonce de plan. Dans un premier temps, afin de démontrer l'idéalisme de la construction juridique pour les données, il est nécessaire d'identifier le cadre normatif. L'analyse des normes permet d'étudier l'appréhension de la notion de données par le Droit. La typologie des différentes notions de données assure une classification des données selon leur origine et leur nature. L'identification des notions sera l'étape préalable indispensable à l'identification des différents régimes juridiques et il conviendra de distinguer les différents régimes juridiques applicables pour chaque type de données. Les régimes juridiques doivent être étudiés au prisme de la régulation mise en place ces dernières années, qu'il s'agisse de la régulation des données à caractère personnel ou des données à caractère non personnel. En tout état de cause, les régimes s'avèrent *a priori* antagonistes au regard des objectifs d'ouverture et de protection des données. L'antagonisme des régimes juridiques rend la cohérence du cadre normatif complexe. Afin de comprendre les facteurs de la complexité du cadre, l'influence des groupes de pression sur l'élaboration des normes ne peut être ignorée (**Partie 1 : L'élaboration d'un cadre normatif complexe).**

Dans un second temps, il est nécessaire d'analyser la mise en œuvre du cadre normatif. Tout d'abord, l'articulation des normes est devenue une opération périlleuse. Avec le développement des technologies émergentes et l'influence des géants du numérique, la hiérarchie des normes est bouleversée. En effet, l'État de droit est bousculé par les nouveaux pouvoirs que constituent les géants du numérique, impactant la marginalisation de l'État dans la construction du cadre normatif au bénéfice d'une certaine prééminence du législateur européen. En parallèle, la privatisation subreptice du système par les principaux acteurs du numérique sera prise en considération. L'ensemble de ces bouleversements remet en cause la cohérence du cadre normatif pour les données. Les pratiques évolutives des géants du numérique ne cessent d'affaiblir l'effectivité des principes mis en place. Par ailleurs, la complexité du régime répressif

et l'insuffisance des sanctions impactent également l'effectivité du cadre normatif (**Partie 2 : La mise en œuvre lacunaire du cadre normatif**).

PARTIE 1 :
L'ÉLABORATION D'UN CADRE NORMATIF COMPLEXE

« Dans la plupart des systèmes de droit, semble-t-il, au nom d'une tendance générale à plus de dirigisme, aboutit à multiplier les textes qui deviennent de plus en plus pointilleux et techniques. La réglementation de détail, si poussée soit-elle, ne peut cependant tout prévoir, alors que des principes généraux peuvent abriter de multiples situations nouvelles et imprévues. Elle conduit à des carences juridiques ou, inversement, à des contradictions entre trop de textes qui se superposent[171]*. »*

39. Annonce de plan. Afin de protéger les individus des pratiques néfastes des géants du numérique, un cadre normatif se construit pour les données. L'antagonisme des objectifs, c'est-à-dire la protection des données à caractère personnel et l'ouverture des données à caractère non personnel aboutit à l'élaboration d'un cadre normatif complexe**.** Dans un premier temps, il convient d'analyser la diversité des notions pour un même objet : les données. Les notions s'avèrent évolutives avec le développement des technologies émergentes et des pratiques des utilisateurs (**Titre 1**). L'identification des différentes normes permet d'analyser les divers régimes juridiques afférents à chaque type de données. Les notions étant d'une diversité excessive, les régimes juridiques sont complexes et divergents (**Titre 2**).

[171] Bergel Jean-Louis, *Théorie générale du droit*, éd. Dalloz, 2012, p. 12.

TITRE 1 : LA DIVERSITÉ ÉVOLUTIVE DES NOTIONS

« Notre temps court est consommateur de droit et d'un droit de plus en plus raffiné, technique, technicien et donc de plus en plus en prise avec des données contingentes. Il y puise une particularité particulièrement pénalisante : c'est un droit à obsolescence programmée[172]*. »*

40. Une discipline vivante. Le droit est une discipline vivante qui nécessite sans cesse de s'adapter à son nouvel environnement. L'environnement numérique bouleverse le droit de par son caractère décentralisé et dématérialisé. Au sein de cet environnement, les flux de données se développent de façon ubiquitaire. Face à l'omniprésence des données, le législateur a appréhendé les données comme un nouvel objet de droit : la « mise en données » du monde ne pouvait être ignorée. Aujourd'hui, les données sont au centre des préoccupations et pourtant, le droit est mis en difficulté pour définir le terme de « données »[173].

41. Des qualifications diverses. La nature des données est protéiforme : les données sont mouvantes et évoluent dans un environnement technique. En pratique, la notion de données ne pouvait faire l'objet d'une unique définition en raison de son polymorphisme. Ainsi, les données sont qualifiées diversement au regard du risque ou du potentiel d'exploitation. L'Union européenne participe également à l'élaboration des définitions afin d'harmoniser le droit des données sur l'ensemble du territoire. En réalité, afin de s'adapter aux technologies émergentes, le droit dérivé et le droit national ne cessent de créer de nouvelles qualifications pour les données, sans pour autant les définir avec précision. Entre les définitions légistiques et les données intégrées par la pratique, les notions sont désormais pléthoriques.

[172] Terré François et Molfessis Nicolas, *Introduction générale au droit*, éd. Dalloz, 2020, p. 423.

[173] Frison-Roche Marie-Anne et Benzoni Laurent, *Internet, espace d'interrégulation*, éd. Dalloz, 2016, p. 7 : « le droit est mis en difficulté parce que le terme de "donnée" assez nouveau, n'est pas aisé à définir. […] Or, le droit est un art pratique qui ne fonctionne bien que s'il manie des catégories dont on maîtrise la définition. ».

42. Annonce de plan. Afin de comprendre de quelle manière le droit a appréhendé la notion de données, il convient de distinguer la notion de « données » de ses notions voisines (**Chapitre 1**), pour pouvoir ensuite analyser les différentes notions juridiques des données (**Chapitre 2**).

Chapitre 1 : La notion de données et les notions voisines : divergences et convergences

43. « Mise en données » du monde[174]. La « mise en données » du monde a été intensifiée par l'émergence des plateformes qui exploitent les données, les interprètent pour les transformer en informations afin de proposer à leurs utilisateurs des services et des contenus toujours plus personnalisés. L'essor des technologies de l'information et de la communication renforce les capacités technologiques afin de transformer les données en informations (**Section 1**), ainsi qu'en contenus numériques (**Section 2**), perturbant les frontières entre les notions de « données », d'« informations », et de « contenus ».

Section 1 : La notion de donnée et la notion d'information

44. Analogies et divergences. Face à l'explosion du volume de données, les technologies liées à l'analyse et l'exploitation des données facilitent leurs transformations en informations. Les sources de données se sont diversifiées et les capacités d'analyses ont évolué. La donnée brute n'a que peu de valeur, c'est son interprétation qui va lui donner un sens afin de construire une information, les deux notions étant assurément proches (I). Pour autant, les deux notions se distinguent au regard de la valeur d'usage de l'information (II).

I. La polysémie des notions

45. Confusion et conséquences. Les définitions des données et de l'information font l'objet de nombreuses déclinaisons, sources de confusion (A). En réalité, les deux notions doivent être distinguées : les données sont le point de départ de la construction de l'information (B).

A) La confusion des notions

46. Analyse des définitions. Les notions de « données » et d'« informations » ne font pas l'objet d'une définition unique. Afin de comprendre la confusion des notions, il est nécessaire

[174] Commission nationale de l'informatique et des libertés, « Le corps, nouvel objet connecté. Du quantified self à la M-Santé : les nouveaux territoires de la mise en données du monde », Cahiers IP, n° 02, mai 2014, p. 3.

d'analyser l'étymologie des notions (1). Récemment, une définition légistique des données a été instaurée (2).

1. L'étymologie des notions

47. Étymologie équivoque des notions. Le terme français « donnée » provient du latin *data* - pluriel de *datum* -, signifiant « chose donnée ». Au niveau étymologique, les données relèvent davantage du donné. Un donné pourrait être ce que l'on n'a pas cherché à posséder, à capturer, mais qui s'offre à nous[175]. Pour autant, le sens courant de « donnée » est trompeur car malgré leur nom, certaines data sont tout sauf données[176]. En effet, c'est un « hasard malheureux de l'histoire » d'utiliser le terme de *datum* plutôt que celui de *captum*. Les informaticiens ou scientifiques captent ou sélectionnent les données, elles ne lui sont pas données[177] : les données sont « captées », « choisies » ou encore « obtenues » par celui qui les collecte[178] . L'information, quant à elle est, au sens étymologique, ce qui donne une forme à l'esprit. Elle provient du latin *informare*, qui signifie « façonner », « former ».

Au regard de l'étymologie des notions, les deux notions sont bien différentes. L'une est le point de départ, une « chose donnée » et l'autre est la possible continuité ; les données pouvant être « façonnées » afin de construire une information.

48. Définition générale des « données ». L'étymologie de la notion de « données » étant équivoque, il en ressort des difficultés de définition[179]. Plusieurs auteurs ont essayé de définir la notion de données. Pour d'aucuns, la donnée est une description élémentaire numérique d'une réalité[180], un élément brut qui n'a pas encore été interprété[181] ou encore l'énoncé numérique d'un

[175] Davadie Philippe et Kempf Olivier, *La donnée n'est pas donnée*, éd. Kawa, 2016, p. 43.
[176] Couderc Lénaïc, « Data, big data, open data », Regards croisés sur l'économie, La Découverte, n° 23, 2018.
[177] Iberkwe-Sanjuan Fidelia, « Vers la datafication de la société », *in* Meyer Vincent (dir.), *Transition digitale*, éd. LEH, 2017, pp. 31-49.
[178] Rivière Pascal, « Qu'est-ce qu'une donnée ? Impact des données externes sur la statistique publique », Courrier des statistiques, n° 5, 2020.
[179] Sénéchal Juliette, « Les interférences entre la politique de protection des consommateurs et la politique du numérique : entre ordre et désordre juridique », *in* Bertrand Brunessen (dir.), *La politique européenne du numérique*, éd. Bruylant, 2023, p. 662.
[180] Abiteboul Serge, *Sciences des données : de la logique du premier ordre à la Toile,* éd. Fayard : Collège de France, 2012, p. 23.
[181] Chaudet Bruno, « Donnée, information, connaissance », Logiques processuelles, 30 mars 2009.

résultat d'observation[182]. Selon l'Association française de normalisation (AFNOR), la donnée est « un fait, une notion ou une instruction représentée sous une forme conventionnelle convenant à une communication, à une interprétation ou à un traitement soit par l'homme, soit par des moyens automatiques[183] ». Dans ces termes, la donnée est toujours définie de manière large, pouvant être une description, un fait ou une mesure. L'élément central de la définition étant la symbolisation dans une forme conventionnelle aux fins de communiquer, d'interpréter ou de traiter[184].

49. Déclinaisons de la définition « information ». À l'instar de la donnée, il existe diverses déclinaisons de la définition de l'information. La notion d'« information » serait d'ailleurs une « notion fuyante[185] ». Lorsque le Professeur Catala évoque tout message communicable à autrui par un moyen quelconque, il renvoie l'information à l'idée d'un message, d'un contenu, ainsi qu'un acte de communication[186]. L'information acquiert de la valeur lorsqu'elle peut atteindre son destinataire et serait obtenue à partir de données collectées, en les organisant et structurant pour en dégager du sens[187]. En réalité, il n'existe pas de définition globale de l'information : l'usage du mot est banalisé sans qu'aucune définition partagée ne soit acquise[188]. Ainsi, il s'agit d'une « notion générique, sous laquelle l'opinion commune range des éléments aussi variés qu'une donnée brute, un savoir-faire, une invention végétale, un secret industriel, une idée, une découverte, une création de forme, un événement d'actualité, une donnée à caractère personnel, etc. : autant de concepts plus précis que celui d'information[189] ».

50. Confusion des notions. En réalité, depuis le début des années 2000, la notion d'information a progressivement substitué la notion de donnée dans le discours juridique[190]. Les

---

[182] Viangalli Francois, « Le concept de données en droit du numérique. Essai de définition. », RDI, n° 202, 1er avril 2023.
[183] Lamizet Bernard et Silem Ahmed, *Dictionnaire encyclopédique des sciences de l'information et de la communication*, éd. Ellipses, 1998, p. 590.
[184] Gaudrat Philippe et Sardain Frédéric, *Traité de droit civil du numérique. Tome 1, Droit des biens*, éd. Larcier, 2015, p. 24.
[185] Vivant Michel, « La privatisation de l'information par la propriété intellectuelle », Revue internationale de droit économique, 2006, pp. 361-388.
[186] Catala Pierre, « Ébauche d'une théorie juridique de l'information », D., 1984, p. 98.
[187] Abiteboul Serge, *op. cit.*, p. 23.
[188] Rivière Pascal, *op. cit*.
[189] Passa Jérôme, « La propriété de l'information : un malentendu ? », Droit & Patrimoine, 2001, n° 91, p. 65.
[190] Vergnolle Suzanne, *L'effectivité de la protection des personnes par le droit des données à caractère personnel*, éd. Larcier, 2022, p. 80.

nombreuses déclinaisons des notions sont sources de confusion : le terme de données supplante le terme d'information, sans en être l'exact synonyme[191]. L'Académie française appuie cette confusion en définissant la donnée comme la représentation d'une information « sous une forme conventionnelle adaptée à son exploitation[192] ». De même pour le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel (RGPD) évoquant les données à caractère personnel en débutant la définition par « toute information[193] ».

Ainsi, les notions de « données » et d' « informations » sont intrinsèquement liées dans certaines définitions. En réalité, les notions partagent certaines caractéristiques : elles sont des biens non rivaux, non excluables et d'une valeur marginale proche de zéro[194]. Pourtant, l'information ne se confondrait ni « avec le message, l'idée, la donnée ou la connaissance […] elle serait une entité à part[195] » : dans cette perspective, l'information se définirait par sa fonction. Récemment, une définition légistique a été instaurée pour les données.

2. Définition légistique des données

51. Définition légistique de la « donnée ». Il aura fallu patienter quarante ans pour parvenir à une proposition de définition légistique des données. En 2022, le Règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 (règlement sur la gouvernance des données) a établi une définition au niveau européen. L'article 2 du règlement définit la donnée comme « toute représentation d'actes, de faits ou d'informations et toute compilation de ces

---

[191] Benabou Valérie-Laure et Zolynski Célia, « Rapport sur les données et contenus numériques », CSPLA, 2018, p. 17.

[192] Dictionnaire de l'Académie française, v° « Donnée ».

[193] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), article 4 : « Toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée "personne concernée") ; est réputée être une "personne physique identifiable" une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale. ».

[194] Poullet Yves, « Les données : des ressources en quête de propriété. Regards sur quelques développements récents en droit européen », *in* De Terwangne Cécile, Degrave Elise, Queck Robert et Dusollier Séverine (dir.), *Law, norms and freedoms in cyberspace. Droit, normes et libertés dans le cybermonde. Liber amicorum Yves Poullet*, éd. Larcier, 2018, p. 265.

[195] Daragon Elise, « Étude sur le statut juridique de l'information », D., 1998, chron., p. 64.

actes, faits ou informations, notamment sous la forme d'enregistrements sonores, visuels ou audiovisuels ». La définition intègre les possibilités de réutilisation des données par le terme « compilation », permettant de prendre en compte les évolutions technologiques sur l'analyse et la compilation des données[196]. Par cette définition, les données seraient la représentation d'une information. Dans le cas où la représentation nécessite une étape de transformation, les données peuvent effectivement être définies comme telles. Le cas contraire, les données doivent être distinguées des informations.

B) La distinction des notions

52. Différences. Les données et les informations sont des notions différentes qui ne peuvent être confondues, en raison de leurs natures ambivalentes (1) et de leurs sources diverses (2).

1. La nature ambivalente des données

53. Distinction des notions. La notion de données est une notion abstraite et l'information peut être considérée d'un niveau d'abstraction supérieur à celui de la donnée. Lorsqu'on se saisit mal d'une notion en droit, les incertitudes apparaissent *de facto.* En réalité, « la clarté des notions est plus un besoin de l'esprit affamé de sécurité qu'une traduction de la réalité complexe des choses[197] ». En pratique, il apparaît que l'information a davantage de valeur que la donnée puisqu'elle est porteuse d'un contenu sémantique plus riche que les données qu'elle intègre. Dans un premier temps, la donnée est purement syntaxique[198] : en dehors d'un certain contexte, il ne sera pas possible d'interpréter les données[199]. Par exemple, un chiffre, un signe, sans contexte n'aura aucun sens et demeurera une donnée brute, sans aucune valeur en l'état. Les données brutes sont des données qui n'ont pas subi de traitement mathématique, humain ou

[196] Cassar Bertrand, « Gouvernance des données », Répertoire IP/IT et Communication, Dalloz, 2022 : « Ce choix lexical est fondé sur une vision informatique du retraitement de l'information, il s'apparente à l'une des opérations permettant de faire émerger de nouvelles données. ».

[197] Demogue René, *Les notions fondamentales du droit privé ; essai critique pour servir d'introduction à l'étude des obligations,* éd. Dalloz, 1911, p. 11.

[198] Poullet Yves, « La "propriété" des données. Balade aux "pays des merveilles" à l'heure du Big Data », *Mélanges en l'honneur de Michel Vivant*, éd. Dalloz, 2020, p. 349 : « la donnée est purement syntaxique et son contenu sémantique est en soi pauvre voire nulle. Elle nait au hasard de nos comportements et saisit un instantané de nos vies : possibilité de connexion entre de telles données par des métadonnées, élaborées par le responsable de traitement ou un tiers, la confrontation de ces données avec d'autres données qui peuvent être anonymes au sein de vastes réservoirs de données qui donne sens et permet notamment d'attribuer un profil à chacun, non en soi, mais en comparaison avec des profils attribués à autrui. ».

[199] Paquet Philippe, *op. cit*.

autre. Les données se transforment en information grâce à un traitement et une mise en contexte. *In fine*, l'information est une donnée structurée et mise en contexte[200] : les données précèdent donc l'information dont elles constituent la matière première[201]. À ce sujet, d'aucuns définissent le *Big Data* comme étant « la constitution et l'exploitation de grandes masses de données dans le but de les transformer en information[202] ». Ainsi, le défi est de transformer les données brutes en informations - c'est-à-dire en données interprétées - afin d'en extraire de la connaissance et d'en tirer du sens[203]. Les notions de données, informations et connaissances ne peuvent donc être confondues puisque la donnée est une matière première de l'information et l'information est une source de la connaissance.

54. Nature ambivalente des données. Les données sont de nature protéiforme puisqu'il existe des données numériques, symboliques, textuelles, logiques, etc. Les données n'ont jamais été un élément naturel, elles sont des produits humains, issues de choix (ou d'absence de choix) politiques, économiques, sociaux, idéologiques, philosophiques ou encore étiques[204]. En effet, le terme de « données » est ambivalent et dont l'acceptation technique renvoie à tous produits digitaux de la numérisation destinés à l'ordinateur. L'acceptation générale du terme renvoie quant à elle à tout objet susceptible de numérisation[205]. D'une façon synthétique, les données peuvent être définies comme « la transcription d'un élément ou d'un phénomène réel en une masse d'informations immatérielles uniquement accessible par un terminal numérique[206] ». À l'état brut, les données sont objectives puisqu'il n'y a pas d'intention dans la donnée.

---

[200] Strowel Alain « Les données, un nouvel actif à l'intersection des propriétés intellectuelles », *in* Bruguière Jean-Michel, *La para-propriété intellectuelle*, éd. Dalloz, 2022, p. 97 : « Une autre façon de distinguer les deux est de considérer les données au niveau syntaxique (en tant que bits d'un système de traitement) et les informations au niveau sémantique (en tant qu'unités chargées de sens). ».

[201] Vergnolle Suzanne, *L'effectivité de la protection des personnes par le droit des données à caractère personnel,* éd. Larcier, 2022, p. 70.

[202] Bensamoun Alexandra et Zolynski Célia, « Big data et privacy : comment concilier nouveaux modèles d'affaires et droits des utilisateurs ? », LPA, 2014, p. 8.

[203] Basdevant Adrien et Mignard Jean-Pierre, *L'empire des données*, éd. Don Quichotte, 2018, p. 14.

[204] Cattaruzza Amaël, *Géopolitique des données numériques : Pouvoir et conflits à l'heure du Big Data*, éd. Le Cavalier Bleu, 2019.

[205] Benabou Valérie-Laure et Zolynski Célia, *op. cit*., p.17.

[206] Cassar Bertrand, « Gouvernance des données », *op. cit*.

2. Les sources des données

55. Sources des données. Avec le phénomène de *Big Data*, au-delà de la quantité de données disponibles, c'est la source même des données qui a changé. Les données sont désormais produites par l'homme ou par des machines, grâce aux capteurs et aux objets connectés. Les données existent depuis longtemps, le bouleversement se trouve dans la manière de pouvoir tout mesurer grâce aux technologies émergentes : « comme l'invention du microscope a ouvert une nouvelle fenêtre sur la nature, les capteurs numériques sont en train de jeter le filet sur le monde pour le rendre mesurable en tout[207] ». Les capteurs enregistrent nos faits et gestes, les smartphones récoltent nos communications, les réseaux sociaux détaillent nos envies et les objets connectés mesurent l'intégralité des actes[208]. Par ailleurs, les objets connectés deviennent des objets « bavards » pouvant communiquer entre eux, créant ainsi des données et métadonnées - structurées ou non -, qui peuvent se transmettre et se reproduire[209]. Ainsi, plus les objets connectés communiquent, plus la masse de données disponible augmente.

Aujourd'hui, les données non structurées peuvent être exploitées et ont une importance croissante. Elles sont plus accessibles, inédites et se présentent sous la forme de « flux »[210]. Le flux des données non structurées se renouvelle en permanence, permettant de maintenir les données à jour. Les données non structurées vont permettre de compléter d'autres données afin que l'homme ou les systèmes puissent transformer l'ensemble de ces données en informations[211].

---

[207] Cardon Dominique, *À quoi rêvent les algorithmes*, éd. Seuil, 2015, p. 8.
[208] Lejeune Yannick, *Big, fast, open data : Décrire, décrypter et prédire le monde : l'avènement des données*, éd. FYP, 2014, p. 11.
[209] Davadie Philippe, *op. cit*.
[210] Bougeard Aurélien, « Le phénomène de Big Data et le Droit, Pour une appréhension juridique par sa décomposition technique », Thèse, Strasbourg, 2022, p. 22 : « Les big data sont la résultante d'une mise en circulation des données dans des flux continus ayant un mouvement concentrique. Une fois donc le big data "créé" et matérialisé en un ou des points de stockage, le mouvement l'alimentant se poursuit, tout en autorisant par la suite une redistribution de nouveaux flux, cette fois-ci vers l'extérieur. ».
[211] Chignard Simon et Benyayer Louis-David, *Datanomics*, éd. FYP, 2015, p. 32.

II. La construction de l'information

56. Usage des données. La notion de valeur des données a en réalité peu de sens, c'est son usage qui lui confère sa valeur (A). Le potentiel de l'usage est exploité par les entreprises dites « traditionnelles » et constitue le cœur du modèle économique des plateformes. L'usage massif des informations peut cependant comporter des risques pour les utilisateurs, souvent inconscients de cet usage (B).

A) L'analyse et l'exploitation des données

57. Transformation des données. L'usage des données va permettre de les analyser et de les interpréter afin de les transformer en informations (1), processus déterminant dans une économie de la donnée (2).

1. L'analyse des données

58. Construction de l'information. Les données brutes n'ont aucune valeur, elles doivent être « nettoyées », « raffinées », afin de pouvoir être utilisées[212]. Lorsque les données sont enrichies, elles seront elles-mêmes une source de métadonnées. Les métadonnées servent à améliorer le traitement sur les données puisqu'elles fournissent des informations sur les données comme le contexte, la structure et la source. L'intérêt de l'informatique étant de pouvoir croiser plusieurs données ensemble afin de donner naissance à l'information : plus la masse de données est importante, plus leur rassemblement et leur croisement permettent de créer de nouvelles données et de construire des informations. Les données peuvent être considérées comme la base d'une pyramide où les données précèdent l'information, qui précède la connaissance : « il y aurait donc un processus de distillations successives à partir de données vers des niveaux supérieurs d'intelligibilité[213] ».

[212] Rouvroy Antoinette et ColinJean-Noël, « Des données et des Hommes. Droits et libertés fondamentaux dans un monde de données massives. », Conseil de l'Europe, 2016, p. 9.
[213] Strowel Alain, « Les données, nouvel actif à l'intersection des propriétés intellectuelles » *in* Bruguière Jean-Michel, *La para-propriété intellectuelle,* éd. Dalloz, 2022, p. 117.

59. Valeur d'usage de la donnée. La notion de valeur des données est équivoque, c'est l'usage des données qui leur confère de la valeur. La valeur des données réside avant tout dans la capacité à les utiliser intelligemment[214]. L'usage va permettre de mesurer un phénomène, d'améliorer la relation avec un client ou un utilisateur, et surtout de pouvoir prendre une décision en temps réel[215]. La décision qui découle de l'analyse des données, c'est-à-dire l'information, a plus d'utilité que les données elles-mêmes. Les données ont donc une valeur subjective, une valeur d'usage ne découlant pas nécessairement des données *per se* mais plutôt de ce qu'elles permettent de faire et des potentielles stratégies auxquelles elles donnent accès[216]. Chaque secteur dispose ou collecte des données choisies à un moment donné. Pourtant des données qui ne sont pas pertinentes lors de la collecte peuvent le devenir plus tard, ou peuvent être réutilisées pour d'autres usages[217]. Il ne suffit pas de détenir un grand nombre de données, il faut aussi savoir les sélectionner, les analyser et les utiliser.

60. Analyse des données. La croissance exponentielle des données et le perfectionnement des capacités d'analyse ont bouleversé les rapports avec l'information[218]. Le phénomène consacre notre entrée dans « la société de l'information[219] ». Jusqu'à récemment, l'exploitation des données était difficile, voire impossible, car les volumes étaient trop importants et les outils techniques d'analyse pas encore inventés[220]. Depuis une dizaine d'années, la création d'une nouvelle génération d'algorithmes permet de gérer ces données de manière plus efficiente, cela grâce à un ensemble de technologies[221]. L'ensemble de ces technologies permet de travailler à partir de données peu structurées, partielles et très souvent incomplètes. À titre d'illustration,

---

214 Frenot Stéphane et Grumbach Stéphane, « Des données à l'intermédiation, une révolution économique et politique. Big data : nouvelles partitions de l'information », *in* Broudoux Evelyne et Chartron Ghislaine (dir.), *Big data, Open data. Quelles valeurs ? Quels enjeux ?*, éd. de Boeck, 2014, pp. 97-120.

215 Marchal Aurélie, « Réflexions sur l'innovation organisationnelle à l'ère du numérique », éd. EMS, n° 7, septembre 2014.

216 Lejeune Yannick, *op. cit*.

217 Rouvroy Antoinette et Colin Jean-Noël, « Des données et des Hommes. Droits et libertés fondamentaux dans un monde de données massives », Conseil de l'Europe, 2016, p. 5.

218 Cardon Dominique, *À quoi rêvent les algorithmes*, éd. La République des idées : Seuil, 2015, p. 15.

219 Zolynski Célia, « Big data : pour une éthique des données », Information, données & documents, 2015, pp. 25-26 : « Le Big data consacre indiscutablement notre entrée dans la société de l'information. Ce terme désigne la capacité à traiter en temps quasi réel d'immenses gisements d'informations, de grandes masses de données structurées, semi-structurées, voire non structurées et disparates pour extraire de leur recoupement de nouvelles valeurs qui demeuraient jusqu'alors inconnues. ».

220 Babinet Gilles et Orsenna Erik, *Big Data, penser l'homme et le monde autrement*, éd. Le Passeur, 2015, p. 21.

221 Derave Charly, Frydman Benoît et Genicot Nathan, *L'intelligence artificielle face à l'État de droit*, éd. Bruylant, 2024, p. 11.

la fouille de données est un processus consacré par le code de propriété intellectuelle comme « la mise en œuvre d'une technique d'analyse automatisée de textes et données sous forme numérique afin d'en dégager des informations, notamment des constantes, des tendances et des corrélations[222] ». La fouille de données ou « data mining » permet donc de transformer des données afin de construire des informations. Cette technique permet de mettre en lumière des modèles statistiques sur des masses de données diversifiées, structurées ou non[223].

61. ***Machine et deep learning.*** Par ailleurs, l'analyse de ces données est également affinée grâce au phénomène du *Big Data.* En effet, le *Big Data* est intiment lié à l'intelligence artificielle : cette technologie repose les données[224]. Les *big data* désignent d'ailleurs de vastes quantités de données numériques, très variées et dynamiques transmises sur des réseaux informatiques et analysés grâce aux nouveaux outils d'analyse[225]. Dans cet univers, ce sont les données qui sont déterminantes et non l'information[226]. La Commission européenne rappelle qu'en l'absence de données, il est simplement impossible de développer des applications d'intelligence artificielle et d'autres applications numériques[227]. L'analyse des données est aujourd'hui facilitée par les techniques dites de *machine learning* et *deep learning*.

Le *machine learning*, autrement dit « apprentissage machine » est un processus par lequel un algorithme évalue et améliore ses performances sans l'intervention d'un programmeur, en répétant son exécution sur des jeux de données jusqu'à obtenir, de manière régulière, des résultats pertinents[228]. Dans ce cas, l'intelligence artificielle est en mesure d'apprendre seule à partir de données catégorisées par l'humain[229]. Aujourd'hui, une partie des informations naît au

---

[222] Code de propriété intellectuelle, article L122-5-3.

[223] Bougeard Aurélien, « Le phénomène de Big Data et le droit », Thèse, Strasbourg, p. 83.

[224] Bertrand Brunessen, « La gouvernance des données dans la régulation européenne de l'intelligence artificielle », RTD eur., 2022, n° 315.

[225] Mayer-Schönberger et Cukier Kenneth, *Big Data. A Revolution that will transform how we live, work and think,* éd. Houghton Mifflin Harcourt, 2013, p. 6.

[226] Strowel Alain, *op. cit*.

[227] Commission européenne, « Intelligence artificielle. Une approche axée sur l'excellence et la confiance », Livre blanc, Bruxelles, 19 février 2020, COM(2020), p. 9 : « sans données, il est impossible de développer des applications d'intelligence artificielle et d'autres applications numériques ».

[228] Journal Officiel de la République Française (JORF), v° « Apprentissage automatique », 9 décembre 2018.

[229] Nevejans Nathalie, « Données et technologies numériques : quels défis pour le XXIe siècle ? », *op. cit*., p. 17 : « Déployée à partir des années 50, l'intelligence artificielle est aujourd'hui en mesure d'apprendre seule à partir de données catégorisées par l'humain (machine learning), et même à partir de données non structurées par l'homme, en identifiant elle-même les caractéristiques discriminantes d'une masse volumineuse de données pour classifier un objet (deep learning). ».

sein des systèmes d'intelligence artificielle[230]. Allant encore plus loin, le *deep learning*, autrement dit « apprentissage profond » correspond à un apprentissage automatique qui utilise un réseau de neurones artificiels composé d'un grand nombre de couches dont chacune correspond à un niveau croissant de complexité dans le traitement et l'interprétation des données[231]. Pour l'analyse des données, les modèles de *machine learning* apprennent davantage avec une masse de données non structurées, endommagées, incomplètes, plutôt qu'avec peu de données structurées et efficaces[232]. Ainsi, les données sont devenues « l'atome » du numérique permettant de nourrir les algorithmes d'intelligence artificielle[233].

62. Potentiel des données. Ces données sont une véritable source d'opportunités dans divers domaines et particulièrement pour la science. La science a besoin de données pour comprendre certains phénomènes et faire évoluer certaines pratiques, notamment en matière d'écologie. À ce titre, le développement des *smart city* ou villes intelligentes permet l'optimisation routière ou la gestion de l'électricité. L'intelligence artificielle va également rendre l'agriculture plus efficiente en augmentant l'efficacité des systèmes de production par la maintenance prédictive et s'adapter au changement climatique[234]. En médecine, l'usage et l'analyse des données de santé vont tout d'abord améliorer les méthodes de recherche scientifique fondées sur les corrélations statistiques[235]. L'intelligence artificielle va plus encore plus loin en instaurant l'aide au diagnostic, à la prescription et à la dispensation. L'intégration de cette technologie en matière de santé promet d'améliorer la précocité et la précision des prises en charge en matière de

[230] Poullet Yves, « La "propriété" des données. Balade aux "pays des merveille" à l'heure du Big Data », *op. cit*.
[231] Journal Officiel de la République Française (JORF), v° « Apprentissage profond », 9 décembre 2018.
[232] Lejeune Yannick, *op. cit*.
[233] Martial-Braz Nathalie, « La transdisciplinarité du droit numérique », *Penser le droit de la pensée : Mélanges en l'honneur de Michel Vivant*, éd. Dalloz, 2020, p. 860.
[234] Castets-Renard Céline, *Droit du marché unique numérique et intelligence artificielle,* éd. Bruylant, 2020, p. 332.
[235]Debiès Élise, « Big data de santé et autodétermination informationnelle », RFAP, n° 167, 2018.

prédiction des maladies[236]. Par exemple, en matière d'imagerie médicale, les algorithmes d'apprentissage automatique peuvent parfois être d'une efficacité supérieure à l'humain[237].

Par-delà ces usages philanthropiques, l'exploitation des données est principalement monopolisée par quelques acteurs du numérique. Ils détiennent une masse impressionnante des données et les utilisent à des fins mercantiles.

2. L'exploitation des données

63. L'usage des données : un intérêt économique majeur. À ce jour, la plupart des entreprises doivent réfléchir à intégrer une stratégie de gestion de l'information dont les données constituent le cœur du modèle d'affaires. La révolution des données a déjà « contaminé » chaque secteur d'activité : le secteur primaire, le secteur secondaire et le secteur tertiaire. Depuis les années 2000, un nouveau secteur prenant en compte les évolutions technologiques est apparu : le secteur quartenaire. La révolution digitale est le passage d'une société industrielle à une société de services. La nouvelle société de service est basée sur les données[238]. En effet, l'intérêt économique des données est devenu incontournable pour toutes les entreprises, même les entreprises dites « traditionnelles »[239]. À l'heure de la « révolution de la donnée[240] », la différence pour une entreprise ne se fait plus sur l'acquisition de données mais sur sa capacité à les traiter et à les utiliser pour prendre des décisions[241]. Les entreprises doivent

---

[236] Voillemet Agathe, « L'exploitation des données de santé dans le cadre de l'intelligence artificielle », *in* Nevejans Nathalie, *Données et technologies numériques*, éd. Mare et Martin, 2021, p. 258 : « D'autre part, l'intelligence artificielle profite au progrès de la santé collective grâce à l'accélération de la recherche, l'identification et l'anticipation des risques sanitaires et la prévention en matière d'épidémiologie ou de pharmacovigilance. L'ensemble de ces avantages mèneront, à terme, à la réduction des dépenses de l'Assurance maladie. Force est de constater que les domaines d'application de l'intelligence artificielle et ses enjeux sont importants. ».

[237] G'Sell Florence, « Les décisions algorithmiques », *in* G'Sell Florence, *Le Big Data et le Droit*, éd. Dalloz, p. 91.

[238] Cointot Jean-Charles, Eychenne Yves, *La révolution du Big Data : Les données au cœur de la transformation de l'entreprise*, éd. Dunod, 2014.

[239] Rouvroy Antoinette et Berns Thomas, « Gouvernementalité algorithmique et perspectives d'émancipation », La Découverte, 2013 : « Les entreprises privées recueillent des quantités de données à des fins de marketing et de publicité, d'individualisation des offres, d'amélioration de leur gestion des stocks ou de leurs offres de service, bref, en vue d'accroitre leur efficacité commerciale et donc leurs profits. ».

[240] Boillet Nicolas, Baranes Edmond, Sauron Jean-Luc *et al.*, « Le règne des données », Cahiers français, 2021.

[241] Paquet Philippe, « De l'information à la connaissance », Cahier de recherche, 2006.

utiliser de manière optimale les données afin d'analyser les besoins masqués ou à venir[242]. Les entreprises doivent transformer ces données en informations afin de pouvoir les utiliser, les exploiter[243]. Ainsi, l'économie devient une société axée sur les données dont elles sont le support des transactions commerciales[244].

64. L'usage des données : un actif stratégique. Avec la collecte massive et l'exploitation de ces données, nous sommes passés d'un « marketing de masse » à un « marketing personnalisé ». Le marketing personnalisé va permettre d'offrir un service plus personnalisé et plus adapté aux besoins en temps réel. Depuis le développement d'Internet, les géants du numérique ont développé des pratiques de captation des données à caractère personnel des utilisateurs[245]. Grâce aux techniques de traitement et d'exploitation des données, ils ont pu mettre en œuvre des techniques de collecte invisible des données afin de récupérer l'ensemble des données de leurs utilisateurs à leur insu[246] : pendant longtemps, leurs pratiques étaient totalement inconnues du grand public[247]. L'insouciance des utilisateurs sur la collecte de leurs données a permis à ces entreprises de faire émerger un nouveau modèle économique[248]. En pratique, Airbnb a ainsi commercialisé chaque soir plus de nuits de sommeil que l'ensemble de l'industrie hôtelière, sans avoir construit aucun hôtel, et tout cela repose massivement sur l'exploitation des données[249]. Les GAFAM ont rapidement compris l'intérêt économique des données et développent sans cesse des nouvelles techniques de traitement, d'agrégation, et d'analyse. D'une façon assez paradoxale, la valeur d'usage de l'offre de services en ligne

[242] Delort Pierre, *Le Big Data*, éd. PUF, 2018, p. 71 : « La "culture données" en entreprises, définie largement comme l'intégration des données dans les décisions et la tolérance aux argumentations fondées sur des données, repose sur une culture quantitative. ».
[243] Jean-Michel Bruguière, *L'émergence d'un droit des données*, éd. Dalloz, 2023, p. 25.
[244] Coudray Chloé et Deffains Bruno, « La construction d'une politique européenne du numérique : enjeux économiques », *in* Bertrand Brunessen (dir.), *La politique européenne du numérique,* éd. Bruylant, 2023, p. 68 : « Les données jouent plusieurs rôles essentiels et très différents dans une société axée sur les données : elles sont le support des transactions commerciales dans l'espace numérique, le capital social essentiel de l'économie axée sur les données et l'infrastructure d'un monde numérisé. ».
[245] Thieulin Benoît, « Gouverner à l'heure de la révolution des pouvoirs », Pouvoirs, 164, 2018, p. 24.
[246] Vergnolle Suzanne, *L'effectivité de la protection des personnes par le droit des données à caractère personnel*, éd. Larcier, 2022, p. 142.
[247] Bourgeois Matthieu et Thibierge Louis, « Droit de la donnée : plaidoyer pour un régime général », La semaine juridique, 2020.
[248] Ho-Dac Marion, « Les données numériques comme biens de consommation. Approche de droit européen des contrats », *in* Nevejans Nathalie (dir.), *Données et technologies numériques,* éd. Mare et Martin, 2021, p. 49.
[249] Babinet Gilles et Orsenna Erik, *op. cit.*, p. 178.

dépend de la production de données par les utilisateurs eux-mêmes[250]. Aujourd'hui, les données sont devenues le pouvoir de marché dans l'économie numérique[251]**.**

65. Les nouveaux acteurs. Afin d'analyser cette quantité de données disponibles, des métiers inédits apparaissent. Il existe désormais des « *data scientist* » pour traiter, analyser et comprendre la donnée, des « *data engineers* » qui manipulent de grande quantité de données et des « *data brokers* »[252]. Les « *data brokers* » ou « courtiers en données » échangent chaque jour des quantités insoupçonnées de données. Ils s'appellent Axciom, BueKai, Rapleaf, Weborama, ou encore Cambrige Analytica parmi tant d'autres[253]. L'objectif de ces courtiers en données est de commercialiser les données à des entreprises afin de mieux cibler leurs clients. Les courtiers de données sont des acteurs importants dans le changement de paradigme du marketing personnalisé.

En pratique, ils ne vendent pas de données brutes, ils les analysent, les agrègent afin de les transformer en informations pertinentes pour les entreprises. Le marché des courtiers en donnée est un marché opaque, peu connu par les utilisateurs. Pourtant, ces entreprises de courtage de données réalisent un chiffre d'affaires qui s'accroît de manière exponentielle, et ce, de manière invisible[254]. L'usage des données est alors une révolution pour les entreprises qui ont les moyens de les exploiter, afin de créer de nouveaux services et de nouveaux produits. Malheureusement, les différents usages comportent des risques pour les individus.

---

[250] Lanna Maximilien, « Les objets connectés : entre remise en question de la notion de vie privée et évolution du droit des traitements des données personnelles », RDP, n° 5, 2017, p. 1435.

[251] Martial-Braz Nathalie, *op. cit*., p. 860.

[252] Lejeune Yannick, *Big, fast, open data*, éd. FYP, 2014.

[253] Suite au scandale, l'entreprise Cambridge Analytica avait annoncé sa fermeture le 2 mai 2018 dans un communiqué.

[254] En 2020, les « data brokers » seraient environ 4000 à réaliser un chiffre d'affaires de plus de 170 milliards.

B) Les risques de l'exploitation des données

66. L'inconscience des utilisateurs. Le modèle d'affaires des géants du numérique repose sur l'exploitation des données de leurs utilisateurs. L'ensemble des données est collecté et analysé afin de personnaliser les services et d'identifier les publicités idoines (1). Toutefois, l'exploitation des données des internautes ne constitue pas seulement un simple échange contre un service gratuit. Les utilisateurs sont souvent inconscients des conséquences néfastes de ce modèle d'affaires (2).

1. Le modèle économique des plateformes

67. Un marché « biface ». Le développement d'une nouvelle économie de services numériques fondée sur l'intermédiation a contribué à généraliser massivement les pratiques de captation des données à caractère personnel des utilisateurs[255]. Le modèle économique de Facebook et Google est un marché biface : d'un côté, ils offrent un service dit « gratuit », et de l'autre, ils revendent les données des utilisateurs à des annonceurs ou à des courtiers en données[256]. L'ensemble des données exploitées sont celles laissées par l'internaute lors de ses navigations sur les plateformes. Dominique Cardon évoque des « signaux » pour identifier les informations livrées activement à un service ou un interlocuteur, l'individu étant conscient de livrer ces informations. En revanche, l'individu laisse également des « traces » en naviguant sur Internet via des traceurs - tels que les clics, géolocalisation, navigation, vitesse de lecture, etc - de manière inconsciente[257]. Les traces peuvent être définies comme « l'enregistrement de toutes les actions d'un individu sous forme de données informatisées[258] ». L'internaute est « tracé » en permanence par son adresse IP, les cookies, les téléphones intelligents, les objets connectés et même les informations collectées hors-ligne (données bancaires, cartes de fidélité, etc.)[259]. L'ensemble des traces des internautes sont alors susceptibles d'être enregistrées,

[255] Vergnolle Suzanne, *op. cit*., p. 143 : « C'est ainsi que les moteurs de recherche mais également les plateformes en ligne, et en particulier les réseaux sociaux génèrent une manne inépuisable de données sur les habitudes, goûts, centres d'intérêts de leurs utilisateurs. ».

[256] Peugeot Valérie, « Données personnelles : sortir des injonctions contradictoires », VECAM, 13 avril 2014.

[257] Cardon Dominique, *op. cit.*

[258] Perriault Jacques, « Traces numériques personnelles, incertitude et lien social », La Revue, 53, éd. CNRS, 2009, pp. 13-20.

[259] Netter Emmanuel, « L'identité numérique », Droit et numérique, 2013 : « La question est plus large encore, puisqu'un traitement numérique est appliqué à des données qui ne sont pas directement dévoilées sur Internet : un paiement par carte bancaire dans une boutique physique, laissant des traces dans les fichiers des banques et des commerçants, ou une déclaration fiscale sur papier, rapidement numérisée et intégrée aux

conservées, et analysées par une multitude d'acteurs[260]. Une grande partie des données sont donc produites ou coproduites par les utilisateurs, soit sciemment ou soit à leur insu[261].

L'ensemble des traces des internautes permet d'améliorer les pratiques de publicité ciblée. En effet, la publicité ciblée est devenue un marché extrêmement rentable pour quelques entreprises du numérique et repose sur des milliards de chiffre d'affaires[262]. Google détient une position quasi monopolistique dans le marché des moteurs de recherche avec plus de 85% du trafic mondial de recherche. La position de Google lui permet de s'attribuer la moitié des parts du marché publicitaire des principaux sites de recherche. En 2023, les revenus publicitaires de Google s'élevaient à 237,86 milliards de dollars[263]. La publicité ciblée est permise grâce aux traces de navigation, collectées à l'aide de *cookies* de suivi permettant aux annonceurs de présenter des publicités personnalisées[264]. Les traces de navigation laissées par les internautes constituent son « patrimoine informationnel[265] ».

68. Un marché « multiface ». En pratique, il est même possible d'évoquer un marché « multiface ». D'un côté, les plateformes publient ou donnent accès à des contenus aux utilisateurs en échange de leurs données à caractère personnel. De l'autre côté, les annonceurs et les publicitaires peuvent bénéficier d'un ciblage commercial affiné avec les données à caractère personnel des utilisateurs[266]. Le développement de ces marchés a permis aux géants

---

fichiers de l'administration, en constituent deux exemples pris au hasard. Or, il semble difficile de distinguer deux avatars numériques dont l'un existerait "en ligne" et l'autre "hors-ligne", car toute information numérisée a aujourd'hui vocation a être intégrée à un réseau et, au moins potentiellement, à circuler. ».

260 Basdevant Adrien et Mignard Jean-Pierre, *op. cit.*, p.15.

261 Rouvroy Antoinette, « Des données sans personne : le fétichisme de la donnée à caractère personnel à l'épreuve de l'idéologie des Big Data », 2014.

262 Adida Axel, « Pour un profilage des données et une personnalisation de la publicité et des services plus transparents pour le consommateur », *in* G'Sell Florence (dir.), *Le big data et le droit*, éd. Dalloz, 2020, p. 274 : « Au quotidien, les technologies publicitaires et de personnalisation sont concentrées autour de quelques plateformes (Google, Facebook, Amazon) et solutions logicielles (Saleforce, Adobe, Oracle). Avec 134,5 milliards de dollars de chiffres d'affaires en 2017, les deux premières plateformes digitales Google et Facebook représentent plus de la moitié du marché du marché de la publicité digitale de 232,27 milliards de dollars. Et l'activité publicitaire d'Amazon, leader de l'e-commerce, a rapidement crû pour atteindre 2 milliards de dollars par trimestre. ».

263 Statista, « Chiffre d'affaires publicitaire de Google 2023 », 22 mai 2024.

264 Commission nationale de l'informatique et des libertés, v° « Cookie » : « Un cookie est un petit fichier stocké par un serveur dans le terminal (ordinateur, téléphone, etc.) d'un utilisateur et associé à un domaine web (c'est à dire dans la majorité des cas à l'ensemble des pages d'un même site web). Ce fichier est automatiquement renvoyé lors de contacts ultérieurs avec le même domaine. ».

265 Féral-Schuhl Christiane, *Cyberdroit*, 8ème édition, éd. Dalloz, 2021, p. 543.

266 Bertrand Brunessen, « La volonté de réguler les activités numériques », RTD eur., 2021, 160.

du numérique de bénéficier d'effets de réseaux et de rendements d'échelles[267]. Aujourd'hui, ils sont en situation de monopole et détiennent la majorité des données de la planète. Pourtant, leurs pratiques sont susceptibles de constituer une nouvelle forme de manipulation marketing ou de surveillance des personnes[268].

2. Les risques pour les utilisateurs

69. La bulle de filtres. Subséquemment à l'économie de l'attention, les dispositifs de captation de l'attention peuvent aboutir à une bulle de filtre informationnelle[269]. En effet, lors de leur navigation, les internautes ne sont pas conscients d'être enfermés dans leur propre « bulle de données ». Le militant Eli Pariser a inventé le concept de la « *filter bubble »,* autrement dit le concept de la « bulle de filtres » [270]. Selon leur profil - par la collecte et l'agrégation de leurs données -, les individus vont obtenir des résultats différents pour une même recherche. Dès lors, la révolution d'accès à l'information n'a plus le même sens si cet accès est conditionné en amont par des choix algorithmiques ; si les algorithmes sont des outils technologiques neutres, leurs usages eux, ne le sont pas[271]. Les plateformes utilisent ces algorithmes afin de proposer aux internautes des résultats, des services et des informations toujours plus pertinents et personnalisés. L'algorithme de Facebook détermine notre fil d'actualité selon nos « j'aime » et nos amis, l'algorithme de Google nous propose des résultats de recherche selon nos recherches précédentes et l'algorithme de Netflix nous propose des films

---

[267] Norodom Anne-Thida, « Être ou ne pas être souverain, en droit, à l'ère numérique », *in* Castets-Renard Céline, Ndior Valère et Rass-Masson Lukas (dir.), *Enjeux internationaux des activités numériques*, éd. Larcier, 2020, p. 27.

[268] Nevejans Nathalie, « Données et technologies numériques : quels défis pour le XXIe siècle ? », *in* Nevejans Nathalie (dir.), *Données et technologies numériques*, éd. Mare et Martin, 2021, p. 20.

[269] Zolynski Célia, Le Roy Marylou et Levin François, « L'économie de l'attention saisie par le droit », Dalloz IP/IT, 2019, 614 : « D'un point de vue plus politique, les dispositifs de captation de l'attention peuvent mener à la constitution d'une bulle de filtre informationnelle et, par conséquent, participent d'un enfermement sociologique qui est assumé par les plateformes elles-mêmes puisque celles-ci créent des "profils", des catégories de population, en mettant activement à jour des constantes sociologiques et des habitus sociaux. ».

[270] Pariser Eli, *The filtre Bubble*, éd. Penguin Group, 2012.

[271] Basdevant Adrien, « La discrimination algorithmique », *in* G'Sell Florence (dir.), *Le Big Data et le Droit,* éd. Dalloz, 2020, p. 244 : « Une start-up britannique Wonga répond ainsi aux demandes de crédit en fonction du moment de la journée où celles-ci sont formulées, permettant ainsi de déterminer si une personne est au chômage ou non. Kreditech, une start-up allemande, répertorie 20 000 sources de données, allant des données de localisation, du graphe social de Facebook aux modalités de navigation sur le Web, pour déterminer sa réponse. L'entreprise ZestFinance prend quant à elle comme critère la vitesse à laquelle les utilisateurs font défiler les conditions d'utilisation de leur site, ou le fait que les candidats tapent seulement en lettres minuscules ou majuscules. ».

selon des utilisateurs qui « nous ressemblent ». Par conséquent, les algorithmes enferment l'internaute dans cette « bulle de filtres » et empêchent toute contradiction avec des opinions diverses ou contradictoires.

70. La prison algorithmique. Pour l'auteur Bill Davidow, il s'agit d'une « prison algorithmique »[272]. L'expression désigne le phénomène d'hyperpersonnalisation induit par l'utilisation de données massives. Par l'enregistrement des traces des internautes, les plateformes utilisent les algorithmes afin de les inciter à agir dans une direction plutôt qu'une autre. La manipulation orchestrée par ces algorithmes peut constituer un risque pour les sujets politiquement sensibles. En effet, plusieurs études démontrent que les individus se détournent de plus en plus des médias de masse au profit des réseaux sociaux et le risque est que ces outils d'information deviennent des outils de confirmation[273]. La problématique de cette manipulation algorithmique est principalement l'inconscience des utilisateurs. Afin d'illustrer cette problématique, Henri Laborit avait soulevé le fait qu'il n'existe pas que « des prisons avec des barreaux, il y en a de beaucoup plus subtiles dont il est difficile de s'échapper parce qu'on ne sait pas qu'on y est enfermé[274]». L'inconscience des utilisateurs peut pourtant avoir de graves conséquences sur la vie des individus.

71. Conséquences pour les individus. En effet, certaines décisions fondamentales sont désormais calculées par des algorithmes. Pourtant, l'idéologie selon laquelle les décisions algorithmiques seraient objectives car fondées sur des machines, et donc plus fiables que les humains, est mensongère[275]. Les algorithmes comportent des biais et sont susceptibles de

---

[272] Davidow Bill, « Welcome to Algorithmic prison », The Atlantic, 20 février 2014.

[273] Farchy Joëlle et Tallec Steven, « De l'information aux industries culturelles, l'hypothèse chahutée de la bulle de filtre », Questions de communication, Éditions de l'Université de Lorraine, 2023 : « La plateforme YouTube a aussi été abondamment étudiée sous l'angle des dérives complotistes auxquelles elle conduit. Chaque jour, le système ingère des milliards de signaux en provenance de ses usagers et les algorithmes de recommandation classent de manière industrielle et sophistiquée les vidéos disponibles pour n'en proposer qu'une poignée à chaque utilisateur. L'algorithme de recommandation Watch Next qui propose à l'usager, en lecture automatique, une vidéo immédiatement après celle qu'il vient de visionner, a fait l'objet des plus vives critiques, mettant en avant sa capacité à amplifier la diffusion de vidéos sensationnelles, clivantes ou complotistes afin de capter dans le temps l'attention des utilisateurs. Le lien entre modèle économique publicitaire nécessitant un fort engagement des usagers et des algorithmes de recommandation privilégiant l'émotion et la conflictualité a été questionné. ».

[274] Laborit Henri, *L'esprit du grenier*, éd. Grasset, 1992.

[275] Poullet Yves, « 20 ans de recherche au CRID : le droit est une toile d'araignée », *Variations sur le droit de la société de l'information*, éd. Bruylant, 2002, p. 13 : « Il est faux de dire que la technologie est neutre. ».

provoquer des discriminations pour les individus[276]. Les algorithmes de recommandation de Netflix ne sont pas déterminants pour la vie d'un individu, en revanche cela peut s'avérer plus problématique lorsqu'il s'agit de l'obtention d'un prêt ou d'une aide sociale. Les banques, les bailleurs ou encore les compagnies d'assurances ont massivement recours aux algorithmes pour se substituer à certaines décisions. L'enjeu est important car ces décisions peuvent potentiellement priver les individus à un crédit, un contrat d'assurance ou un contrat de bail[277]. La technique du « scoring » visant à collecter des données sur les futurs clients afin de sélectionner sur le fondement d'un algorithme le meilleur profit s'est généralisée ces dernières années[278].

[276] Pons Ronan et Risser Laurent, « Biais et discriminations dans les systèmes d'intelligence artificielle », Dalloz IP/IT, 2022, pp. 75-78 : « Pour les connaisseurs, cette illusion a volé en éclats depuis bien longtemps. Les affaires publiques de discriminations réalisées au travers de systèmes automatisés sont désormais nombreuses. Outre dans le célèbre cas du logiciel américain Compas, la présence de biais raciaux a été identifiée dans les logiciels d'identification faciale et plus récemment dans l'attribution des allocations familiales aux Pays-Bas. ».

[277] « Décisions automatisées et profilage », *in* Bensamoun Alexandra, Bertrand Brunessen et Anca Ailincai Mihaela (dir.), *Le règlement général sur la protection des données*, éd. Mare et Martin, 2020, p. 193.

[278] Legeais Dominique, « Scoring. Encadrement de la technique du score par la Commission nationale de l'informatique et des libertés », RTD com., 2007, 208 : « Le score est une technique largement utilisée principalement pour l'octroi des crédits à la consommation. La technique permet d'identifier les bons clients, ceux qui ont un profil garantissant un remboursement du crédit sans difficultés. Inversement, la technique permet de déceler et donc d'exclure les clients à risques. Un mauvais score signifie ainsi souvent un refus du crédit ou l'octroi d'un crédit à un taux très élevé. ».

72. Conclusion de la section. Les notions de « données » et d'« informations » sont des notions intrinsèques et non des synonymes. Les données constituent le point de départ pour la construction d'une information. Lorsque les données sont enrichies, complétées, mises en contexte, elles deviennent des informations : en ce sens, les informations sont des données structurées.

Afin d'être source de valeur, les données vont devoir être utilisées par les entreprises grâce aux outils d'analyse. Les technologies émergentes permettent de faire évoluer les outils d'analyse afin de les parfaire et de transformer davantage de données en informations. En pratique, les données n'ont pas de valeur intrinsèque : la valeur des données dépend de leurs usages. Avec la masse de données ainsi que les moyens techniques disponibles, les données sont devenues un actif stratégique majeur.

Les géants du numérique ont été pionniers dans la récolte et l'exploitation des données. La masse de données qu'ils possèdent leur permet aujourd'hui d'entraîner de puissants algorithmes afin d'analyser toujours plus de données. L'analyse des données permet d'offrir aux utilisateurs des services personnalisés. Principalement, les outils d'analyse servent à développer la publicité ciblée, marché détenu en partie par Google. En réalité, les données constituent le cœur du modèle d'affaires de ces sociétés.

Pour autant, le monopole des géants du numérique sur les données entraîne des risques pour les utilisateurs qui ne sont pas - la plupart du temps - conscients du marché de leurs données. En effet, l'analyse de données dans un but mercantile peut avoir des effets significatifs sur la vie des utilisateurs.

Par ailleurs, les géants du numérique participent également à la diffusion et la création de contenus. Afin de comprendre le rôle des plateformes sur les contenus, il convient d'analyser les notions de contenus et de données.

Section 2 : Les notions de données et de contenus

73. Le marché des contenus. Grâce au numérique, de nouveaux acteurs sont entrés sur le marché des contenus et des données : les plateformes. Les plateformes exploitent et produisent une quantité considérable de contenus de différentes natures. Les contenus sont des données interprétées et permettent aux plateformes d'augmenter leurs revenus grâce à la publicité ciblée. Dès lors, les plateformes ont tout intérêt à identifier les contenus les plus pertinents pour leurs utilisateurs en fonction des données analysées. En ce sens, les contenus sont une ressource positive pour les plateformes (I). Néanmoins, la dynamique de diffusion des contenus a également suscité des inquiétudes : les contenus diffusés ou échangés peuvent être illicites. Ainsi, le droit s'est saisi de la notion du contenu illicite afin de trouver un équilibre entre la liberté d'expression et le contrôle répressif nécessaire à la sécurité des utilisateurs (II).

I. La notion positive de contenu : des données interprétées

74. Nouveaux usages. Les nouveaux services numériques des plateformes ont bouleversé la diffusion des contenus. Les géants du numérique sont devenus des acteurs incontournables en matière d'ordonnancement et de diffusion des contenus. À l'instar de l'exploitation des données, les plateformes exploitent la valeur des contenus (A). En réalité, les acteurs du numérique s'approprient cette valeur et bouleversent la répartition traditionnelle des gains, entraînant un déplacement de la valeur (B).

A) La valeur des contenus

75. Notion de contenu. La notion de contenu numérique est présente dans divers textes juridiques sans pour autant être réellement définie (1), présence qui démontre l'intérêt des contenus dans ce nouvel univers numérique (2).

1. La polysémie de la notion de contenu

76. Approche usuelle de la notion. Dans un dictionnaire usuel, la notion de « contenu » est définie comme « ce qui est exprimé dans un texte, un énoncé, sa teneur, sa signification[279] ». En réalité, d'aucuns considèrent que la notion de contenu se caractérise par « une absence de définition ou par des définitions lacunaires[280] » ou encore comme une « nouvelle notion juridique floue, située quelque part entre les biens et les services[281] ».

77. Approche juridique de la notion. La notion de contenu apparaît pour la première fois en droit des communications électroniques avec la Directive 2002/21/CE du Parlement européen et du Conseil du 7 mars 2002 relative à un cadre réglementaire commun pour les réseaux et services de communications électroniques énonçant la nécessité de séparer la réglementation de la transmission de celle des contenus[282]. Par la suite, le principe de neutralité d'internet a fait référence à un principe d'égalité de traitement des contenus par les opérateurs de communications électroniques. Enfin, la notion a été introduite en droit de la consommation par la Directive 2011/83/UE du Parlement européen et du Conseil du 25 octobre 2011 relative aux droits des consommateurs, modifiée récemment par la Directive 2019/770/UE du Parlement européen et du Conseil du 20 mai 2019 relative à certains aspects concernant les contrats de fourniture de contenus numériques et de services numériques.

A l'instar de la notion de donnée, la notion de contenu est omniprésente et pourtant, rarement définie. La directive 2019/770 définie le contenu numérique comme « des données produites et fournies sous forme numérique[283] », à l'instar de la directive de 2011, « renvoyant à la notion

---

279 Dictionnaire Larousse, v° « Contenu ».

280 Benabou Valérie-Laure et Zolynski Célia, « Rapport sur les données et contenus numériques », CSPLA, p. 30.

281 Benabou Valérie-Laure et Rochfeld Judith, *À qui profite le clic ?*, éd. Odile Jacob, 2015, p. 33.

282 Directive 2002/21/CE du Parlement européen et du Conseil du 7 mars 2002 relative à un cadre réglementaire commun pour les réseaux et services de communications électroniques, considérant 5 : « Il est nécessaire de séparer la réglementation de la transmission de celle des contenus. Ce cadre ne s'applique donc pas aux contenus des services fournis sur les réseaux de communications électroniques à l'aide de services de communications électroniques, tels que les contenus radiodiffusés, les services financiers et certains services propres à la société de l'information, et ne porte donc pas atteinte aux mesures relatives à ces services qui sont arrêtées au niveau communautaire ou national, conformément au droit communautaire, afin de promouvoir la diversité culturelle et linguistique et de garantir la défense du pluralisme des médias. ».

283 Directive (UE) 2019/770 du parlement européen et du conseil du 20 mai 2019 relative à certains aspects concernant les contrats de fourniture de contenus numériques et de services numériques, article 2.1.

elle-même vaste et non définie de "données", et suggérant que tout ce qui est numérique est un contenu numérique au sens de ce texte[284] ». La notion de contenu numérique est définie sans distinction de la nature du contenu. Le considérant 19 de la directive 2019/770 illustre cette définition par plusieurs exemples comme les fichiers vidéo, les fichiers audios, les applications ou encore les livres électroniques[285]. La directive distingue les services et les contenus numériques, ce qui revient à considérer le contenu numérique comme l'objet du service[286]. La définition est large afin de s'adapter aux progrès technologiques rapides[287].

78. Approche essentialiste de la notion de contenu. En réalité, la définition du contenu est également une notion fuyante. La professeure Valérie-Laure Benabou relève cependant que la notion de contenu numérique est essentiellement tournée vers des contenus à caractère culturel au regard du considérant 19. Dans son article « Entrée par effraction d'une notion juridique nouvelle et polymorphe : le contenu numérique[288] » elle consacre une approche essentialiste de la notion de contenu numérique en identifiant les éléments déterminants du contenu numérique : le caractère non-rival de l'objet numérique et la valeur du contenu. Pour le caractère non-rival, cela revient aux propriétés des choses numérisées dont la particularité est d'être transmise par une opération de reproduction. Le caractère non rival du contenu numérique permet au contenu numérique d'être utilisé par plusieurs utilisateurs, sans réduire l'utilité des autres. Pour la valeur

[284] Benabou Valérie-Laure et Zolynski Célia, *op. cit*.

[285]Directive 2019/770, *op. cit*., considérant 19 : « La présente directive devrait permettre de traiter les problèmes concernant différentes catégories de contenus numériques et de services numériques, et leur fourniture. Afin de s'adapter aux progrès technologiques rapides et de préserver le caractère évolutif du concept de contenu numérique ou de service numérique, la présente directive devrait couvrir, entre autres, les programmes informatiques, les applications, les fichiers vidéo, les fichiers audio, les fichiers musicaux, les jeux numériques, les livres électroniques ou les autres publications électroniques, de même que les services numériques qui permettent la création, le traitement ou le stockage de données sous forme numérique, ainsi que l'accès à celles-ci, y compris les logiciels à la demande, tels le partage vidéo et audio et les autres formes d'hébergement de fichiers, les traitements de texte ou les jeux proposés dans l'environnement informatique en nuage et les médias sociaux. ».

[286] Anciaux Nicolas, Pucheral Philippe, Behar-Touchais Martine, Benabou Valérie-Laure, Brunaux Geoffray, *et al.,* « Contenus numériques », Dossier, 2017.

[287] Zolynski Célia, « Contrats de fourniture de contenus et de services numériques. À propos de la directive (UE) 2019/770/UE du 20 mai 2019 », La Semaine Juridique Édition Générale, n° 47, 18 novembre 2019, 1181 : « Les deux notions de contenus et services numériques sont désormais distinguées, étant entendu que le texte en retient une conception large et met l'accent sur leur caractère fortement évolutif compte tenu des progrès technologiques rapides. Leur définition est illustrée par différents exemples parmi lesquels les programmes informatiques, les applications, les fichiers vidéo, les fichiers audio, les fichiers musicaux, les jeux numériques, les livres électroniques ou les autres publications électroniques ».

[288] Benabou Valérie-Laure, « Entrée par effraction d'une notion juridique nouvelle et polymorphe : le contenu numérique », Dalloz IP/IT, 2017.

de référence du contenu, « elle varie essentiellement en fonction de la valeur des données véhiculées et des utilités consenties sur ces données. […] La valeur du contenu est éminemment dépendante de la qualité de la donnée au regard de l'attente [289]. ».

79. Approche technique de la notion de contenu. En réalité, le contenu numérique est inhérent à l'architecture d'Internet, le terme contenu désignant ici « toute information numérisée accessible via le protocole Internet, quel que soit son sous-jacent[290] ». Le sous-jacent du contenu désigne la finalité de l'information. Le contenu peut alors être défini comme « toute information mise en ligne ayant une finalité autre que d'assurer la transmission des signaux (signalisation) et la délivrance d'un service (logiciel, algorithmes, etc.). Les contenus numérisés peuvent être produits par des individus, des entreprises, des institutions non marchandes, des objets (capteurs), à des fins de communication ou de diffusion, à titre gracieux ou onéreux, directement ou indirectement[291]. ». *In fine* et techniquement, les contenus sont des données interprétées, à forte valeur ajoutée intégrant et mobilisant l'utilisateur[292].

Les données sont la matière première incontournable pour les produits et les services de contenu numérique[293]. D'une certaine façon, il est possible d'affirmer que tous les contenus sont des données. Ainsi, les contenus présentent un intérêt économique majeur pour les plateformes.

2. L'intérêt économique des contenus

80. La nature des contenus. Avec le développement d'Internet, il existe un phénomène de surproduction des contenus en raison des coûts réduits de publication. La surproduction de contenus profite aux plateformes, qui diffusent ces contenus de différente nature[294]. Il peut

---

289 *Ibid*.

290 Benzoni et Dutru, « De l'accès aux infrastructures à l'accès aux moyens numériques : Nouvelle frontière pour la régulation des communications électroniques », *in* Frison-Roche Marie-Anne, *Internet, espace d'interrégulation*, éd. Dalloz, 2016, p. 25.

291 *Ibid*, p. 33.

292 Favro Karine, *Droit de la régulation des communications numériques,* éd. LGDJ, 2018, p. 123.

293 Michéa Frédérique, « L'appréhension de la donnée en droit de l'Union européenne », *in* Nevejans Nathalie, *Données et technologies numériques*, éd. Mare et Martin, 2021, p. 30.

294 Rebillard Franck et Smyrnaios Nikos, « Les infomédiaires, au cœur de la filière de l'information en ligne », Réseaux, La Découverte, 2010 : « Il [le phénomène de surproduction] se double en outre d'une composante nouvelle, liée au caractère archivable et semi-public des échanges informels entre internautes. Tous ces éléments s'additionnent pour former au final un vaste ensemble de productions discursives

s'agir de contenus protégés par un droit de propriété intellectuelle, d'informations relatives à l'actualité, d'informations personnelles concernant un internaute ou encore d'informations relatives à un historique de navigation en ligne. Les contenus numériques peuvent aussi se présenter sous forme de services, comme ceux de *streaming* de film en ligne ou de *cloud* permettant de stocker les données. Le développement des intelligences artificielles génératives renouvelle également la nature des contenus en créant des contenus textuels, graphiques ou audiovisuels[295].

Les notions de « données » et d'« informations » s'intègrent alors dans la notion de contenu. En effet, les données et informations sont intimement liées, elles composent les contenus mis à la disposition des internautes par les plateformes[296]. Le numérique permet de rendre accessible des contenus auparavant exclusivement disponibles de manière matérielle. La nature des contenus numériques devient donc très polymorphe. Pour autant, afin d'acquérir de la valeur, les contenus doivent être diffusés massivement auprès des internautes.

81. Le contenu, source de valeur. Pour être réellement une source de valeur, à l'instar des données et face à la masse d'informations disponible, le contenu doit être trié, classé, identifié et facilement accessible pour l'internaute[297]. La valeur du contenu est directement liée à sa visibilité : qu'importe la valeur du contenu s'il n'est pas visible. Pour ce faire, de nouveaux « services numériques » se sont développés. Les services peuvent fonctionner en collectant les données des internautes et des contenus culturels comme les plateformes vidéo. Puisque la valeur du contenu est liée à sa visibilité, certains services vont rassembler, agréger, trier les informations pour les rendre accessibles aux internautes[298]. Il s'agit pour eux de collecter le maximum de contenus afin de rendre l'offre attractive.

---

numérisées, en s'inscrivant plus largement dans un procès d'informationnalisation qui rend d'autant plus nécessaires des dispositifs de repérage dans ces volumes considérables et hétérogènes de données. ».

[295] Journal Officiel de la République Française (JORF), n° 0212, v° « Intelligence artificielle générative », 6 septembre 2024.

[296] Dejean-Ozanne Christophe, « Économie de la donnée et plateforme en ligne », Thèse, Toulouse 1, 2019, p. 32.

[297] Benabou Valérie-Laure et Rochfled Judith, *op. cit.*, p. 149.

[298] Thuillas Olivier et Wiart Louis, « Plates-formes culturelles : quelles alternatives aux géants du numérique ? », Nectart, n° 8, Éditions de l'Attribut, 2019.

82. La diffusion de contenu par les plateformes. Le fait que les contenus soient désormais accessibles de manière numérique permet à ces plateformes d'héberger et d'agréger les contenus disponibles sur Internet afin de les rendre disponibles. De surcroît, grâce à l'information numérisée, les supports et médias de l'information ne sont plus distincts mais accessibles par les mêmes canaux. Les plateformes ne cessent de diversifier leurs services afin de toujours diffuser plus de contenus. En effet, les plateformes agrègent et traitent l'information afin de diffuser des contenus pertinents et personnalisés tout en se rémunérant grâce à la publicité ciblée[299] : plus le contenu est pertinent, plus les plateformes sont rémunérées par la publicité ciblée et l'exploitation des données à caractère personnel des utilisateurs. Avec l'aide des algorithmes, les plateformes proposent donc des contenus toujours personnalisés aux utilisateurs, afin de capter au maximum leur attention et surtout, de maximiser leurs revenus. Ainsi, grâce à leur maîtrise des données et des algorithmes, les plateformes jouent un rôle primordial dans la diffusion des contenus. Ils arrivent à sélectionner l'information pertinente selon les préférences supposées de l'internaute pour diffuser les contenus idoines.

83. Infomédiaires. Les géants du numérique deviennent des « infomédiaires », c'est-à-dire des intermédiaires qui diffusent *a priori* gratuitement les contenus[300]. Les infomédiaires constituent et contrôlent de vastes silos de données[301]. Grâce à l'ensemble des données, ils classent les contenus d'actualité afin de proposer aux internautes une information personnalisable[302]. À ce jour, Google exerce une domination sans partage en matière d'accès et de diffusion de contenus en ligne, avec une part de marché de 90% en Europe[303]. Google n'est

---

[299] Cluzel-Métayer Lucie, « Contrôler les contenus ? », Pouvoirs, 185, Le Seuil, 2023, pp. 111-122 : « Sous une apparence de gratuité trompeuse, la grande majorité de ces plateformes se financent par la publicité ciblée et par la monétisation des données personnelles de leurs utilisateurs ; il s'agit ainsi, pour la plupart, d'entreprises américaines à but lucratif. Par-delà leur grande diversité, elles fonctionnent toutes sur l'économie de l'attention. ».

[300] Bérard-Quélin Bernard, « La naissance d'un droit voisin au profit des éditeurs et agences de presse », Légipresse, 2019, 107.

[301] Zolynski Célia, « Un nouveau droit de propriété intellectuelle pour valoriser les données : le miroir aux alouettes ? », Dalloz IP/IT, 2018, 94.

[302] Rebillard Franck et Smyrnaios Nikos, *op. cit*.

[303] Smyrnaios Nikos, « L'effet GAFAM : stratégies et logiques de l'oligopole de l'internet », Communication & langages, 188, 2016 : « Dans le domaine de l'actualité, Google et Facebook sont les deux plus gros pourvoyeurs de trafic pour les sites d'information : ils totalisent plus de deux tiers du trafic entrant en moyenne en France comme aux États-Unis. Ils deviennent ainsi indispensables aux éditeurs de presse, qui se trouvent dans l'obligation de se conformer à la fois à leurs exigences économiques et à leurs règles techniques. Google (grâce à YouTube) et Facebook dominent également le marché de la vidéo en ligne. Ce marché est stratégique car il correspond au segment publicitaire de l'internet le plus dynamique. La publicité

pourtant pas la seule plateforme à profiter de la diffusion des contenus. Les géants du numérique s'emparent de la valeur créée sur le web par les internautes, les créateurs et les producteurs.

B) Le déplacement de valeur

84. Participation à la valeur. Dans ce nouvel univers numérique, les internautes participent à la création de valeur en produisant ou en partageant des contenus (1), nouvelle source de valeur capturée par les plateformes (2).

1. La contribution de la valeur par les internautes

85. L'essor du « Web 2.0 ». Dans les années 2000, l'avènement du « *web 2.0* » fondé sur l'interactivité des internautes a bousculé le fonctionnement de l'Internet. Des plateformes comme Twitter, Facebook, Youtube, Amazon, Wikipédia partagent le point commun d'héberger des contenus produits par les usagers. Google le partage aussi - d'une certaine manière - en collectant et traitant des contenus créés par la masse des usagers pour classer les sites en fonction de la topologie des liens hypertextuels. Les plateformes, au lieu de produire du contenu, vont se concentrer sur la mise à disposition d'une architecture de participation, de telle sorte que les usagers puissent créer gratuitement des contenus et par conséquent de la valeur[304].

86. L'internaute, nouveau contributeur de valeur. Avec l'essor de ce web participatif, les internautes sont devenus des acteurs à part, jouant un rôle actif dans la création et la diffusion de contenus. Les internautes vont créer, en permanence, une masse de contenus sans aucun but lucratif[305]. Ils vont diffuser des contenus avec différents moyens techniques comme le téléchargement à partir d'un logiciel de pair à pair[306], le *streaming* et le téléchargement direct[307]. Les internautes sont devenus des sources passives et actives de contenus informationnels : ils

---

en ligne est partagée principalement entre Google et Facebook, qui disposent chacun de points forts respectivement dans les liens sponsorisés et le display. ».

[304] Bénel Aurélien, « 15 ans de Web 2.0 : Imitation pop ou extension du domaine de l'Hypermédia ? », 15ème édition de la conférence Hypertextes et hypermédias, produits, outils et méthodes, 2019, pp. 111-125.

[305] Colin Nicolas et Verdier Henri, *L'Âge de la multitude*, éd. Armand Colin, 2012, p. 98.

[306] Dictionnaire Larousse, v° « peer to peer » : « Technologie permettant l'échange direct de données entre ordinateurs reliés à Internet, sans passer par un serveur central. ».

[307] Netter Emmanuel, *Les biens numériques*, éd. CEPRISCA, 2015, p. 210.

les reçoivent et peuvent se contenter de les consommer, mais ils sont également capables de les commenter, de les modifier et de les retransmettre à leur tour. Ils détiennent un rôle particulièrement actif dans la création, la diffusion et la transformation des contenus[308]. Le modèle passif de l'internaute a laissé place à un modèle actif, contributeur de valeur.

2. La captation de la valeur par les plateformes

87. Les « données sémantiques ». À chaque instant, la valeur créée par l'internaute va être captée par les plateformes numériques : elles ont compris à quel point il était plus confortable de capter des contenus générés et partagés par les utilisateurs plutôt que de payer des équipes chargées de créer ces contenus[309]. Les plateformes ne se limitent pas à capter l'activité créatrice des individus mais également les données dites « données sémantiques sur un contenu ». Les données sémantiques sur un contenu sont les données agrégées à partir de propos des internautes recueillis sur divers sites *Web*[310]. Les internautes vont exprimer leur avis de manière explicite sur des sites dédiés ou de manière implicite sur les réseaux sociaux.

Lorsque les plateformes agrègent ce type de données, elles recueillent des informations précieuses sur la réception des contenus. Grâce à ces données, Amazon revendique 40% de ses ventes avec son moteur de recommandation et Netflix en revendique 60% : ces entreprises s'approprient une valeur construite sur l'analyse intelligente des traces d'utilisation laissées par les millions d'utilisateurs[311]. À partir de ces traces d'utilisation, les plateformes sont capables de connaître et d'interpréter le comportement des utilisateurs afin de leur proposer des services et contenus personnalisés : c'est le développement du « *Web 3.0* », appelé « web sémantique » ou encore « web des données[312] ».

---

[308]Chopin Frédérique, « Responsabilité pénale des fournisseurs de contenu », Répertoire IP/IT et Communication, Dalloz, 2024 : « Si à l'origine, les éditeurs non professionnels étaient essentiellement constitués de particuliers qui créaient un site internet, ou participaient à un webforum en dehors de tout cadre professionnel, l'arrivée du web participatif a changé considérablement les choses. En effet, les forums existent dans tous les domaines, il faut y ajouter les blogs mais aussi et surtout tous les services interactifs et contributifs que sont les réseaux sociaux, les plateformes de partage audiovisuelle, les sites de ventes aux enchères ou de petites annonces. ».

[309] Colin Nicolas et Verdier Henri, *op. cit,* p. 27.

[310] Farchy Joëlle et Denis Juliette, *La culture des données*, éd. Presse des mines, 2020, p. 46.

[311] Colin Nicolas et Verdier Henri, *op. cit*.

[312] Teresi Laurent, « L'open data et le droit de l'Union européenne », AJDA, 2016, 87.

88. Le déplacement de valeur. Au sein de cet espace, les nouveaux services numériques ont bouleversé la répartition traditionnelle des gains sur les contenus : les profits des créateurs de contenus sont remis en question, les internautes ne touchent rien sur l'exploitation de leurs données à caractère personnel, à l'instar des collaborateurs d'œuvres contributives. Les gains de ces contenus et données sont captés directement par les plateformes numériques et ne cessent d'augmenter chaque année. Il existe une réelle problématique de répartition de la valeur entre créateurs ou producteurs et services numériques : « la valeur des créations de l'esprit passe progressivement des mains des créateurs et des producteurs à celles de ces intermédiaires d'un genre nouveau, non impliqués dans le circuit de redistribution relevant du système du droit d'auteur[313]». Les œuvres dans l'univers numérique sont devenues très facilement reproductibles, soulevant des problématiques en matière de propriété intellectuelle.

89. L'ordonnancement des contenus. La captation de la valeur des contenus des internautes a permis à ces plateformes de devenir des acteurs systémiques ou encore des plateformes qualifiées de structurantes[314]. Les plateformes sont donc en mesure de contrôler le marché numérique dans son ensemble : la maîtrise de leur environnement et des contenus sur leur plateforme permet à ces acteurs de pratiquer un ordonnancement subjectif. En effet, les réseaux sociaux définissent un ordonnancement des contenus qui repose sur l'analyse des données relationnelles issues de l'activité du réseau[315]. En pratique, ils vont pouvoir limiter la diversité des contenus et influencer les opinions publiques.

Malheureusement, les contenus à fort engagement sont des contenus principalement illicites. Depuis le développement des réseaux, énormément de contenus illicites se propagent sur les plateformes. Afin de protéger les individus contre les dérives des contenus disponibles sur les plateformes, le législateur instaure et développe la notion de contenus illicites dans le dessein de responsabiliser les géants du numérique.

[313] Benabou Valérie-Laure et Rochfeld Judith, *op. cit*.
[314] Chemain Régis, « La relation juridique des GAFA avec l'Union européenne », Rev. UE, 2023, 90.
[315] Favro Karine, « La lutte contre les stratégies d'influence et les ingérences », *in* Bertrand Brunessen et Le Floch Guillaume (dir.), *La souveraineté numérique*, éd. Bruylant, 2024, p. 208.

II. La notion négative de contenu : les contenus illicites

90. Intégration de nouvelles notions. Depuis quelques années, les plateformes ont pris une place nouvelle et incontournable dans la diffusion des contenus numériques. Afin de lutter contre les contenus illicites, il était indispensable de définir les notions de « contenus haineux » et de « contenus caractère terroriste » (A), ainsi que la notion générique de « contenus illicites » (B).

A) Les notions de contenus haineux et à caractère terroriste

91. Diffusion des contenus litigieux. Il existe une réelle problématique de diffusion des contenus litigieux sur les plateformes. Afin d'identifier de manière pertinente ces contenus, il convient de définir les contenus à caractère terroristes (1) ainsi que les contenus haineux (2).

1. Les contenus à caractère terroriste

92. Définition large du contenu à caractère terroriste. Le terrorisme a trouvé dans l'espace numérique un terrain fertile pour renouveler ses modes d'action[316]. La diffusion de contenus terroristes peut être un catalyseur de la radicalisation des personnes menant à des actes terroristes[317]. Cette diffusion peut donc avoir de graves conséquences sur les utilisateurs, les citoyens et la société[318]. Au regard du rôle central des plateformes dans la diffusion, il devenait nécessaire de les responsabiliser afin de lutter contre les contenus à caractère terroriste diffusés par l'intermédiaire de leurs services en ligne. Pour ce faire, une définition du contenu à caractère terroriste a été instaurée par le législateur. Le règlement relatif à la lutte contre la diffusion des contenus à caractère terroriste en ligne du 29 avril 2021 constitue l'un des premiers textes ayant pour objectif de lutter contre les contenus en ligne[319].

---

316 Lequette Suzanne, *Droit du numérique,* éd. LGDJ, 2024, p. 163 : « S'il est concevable que l'acte terroriste se réalise par voie numérique, notamment en prenant la forme d'une cyber-attaque, c'est davantage en pratique au stade du processus préparatoire de l'acte terroriste que la technique numérique est sollicitée. Elle contribue ainsi à faciliter l'organisation de l'acte : d'une part en fournissant de nouvelles sources de financement, notamment grâce à l'usage des crypto-monnaies ou par l'organisation de commerces illicites sur le dark web ; d'autre part en offrant des canaux de communication permettant de coordonner des moyens humains à une échelle mondiale et de façon secrète. ».

317 Ségur Philippe, « Le terrorisme et les libertés sur l'internet », ADJA, 2015, 160.

318 Règlement (UE) 2021/784 du 29 avril 2021 relatif à la lutte contre la diffusion des contenus à caractère terroriste en ligne, considérant 5.

319 Règlement (UE) 2021/784 du 29 avril 2021 relatif à la lutte contre la diffusion des contenus à caractère terroriste en ligne.

Selon la définition instaurée, il peut s'agir d'un contenu incitant à la commission d'une infraction terroriste - par exemple en glorifiant ces actes - ou de contenus qui sollicitent une personne ou plusieurs personnes pour participer aux activités d'un groupe terroriste, comme la direction d'un groupe terroriste ou la participation aux activités de ce groupe en fournissant des informations ou des moyens matériels[320]. La définition englobe également la menace de la commission d'une infraction terroriste.

Par ailleurs, la définition s'étend au contenu fournissant des instructions concernant la fabrication ou l'utilisation explosifs, d'armes à feu ou d'autres armes, ou de substances nocives ou dangereuses, concernant d'autres méthodes ou techniques spécifiques, aux fins de commettre ou de contribuer à une infraction terroriste. Les autres méthodes comprennent par exemple la fabrication de substances chimiques, biologiques, radiologiques et nucléaires ou concernant d'autres méthodes spécifiques ou techniques spécifiques, y compris le choix de cibles, aux fins de la commission ou de la contribution à la commission d'infractions terroristes. Le matériel intègre des textes, des images, des enregistrements sonores et des vidéos, ainsi que des transmissions en direct d'infractions terroristes, qui entraînent un risque que d'autres infractions de ce type soient commises[321].

93. Exclusion de la définition. En revanche, le matériel diffusé à des fins éducatives, journalistiques, artistiques ou de recherche, ou à des fins de sensibilisation contre les activités terroristes est exclu de la définition. La difficulté résulte dans l'appréciation des contenus de manière objective et non subjective : en effet, les utilisateurs peuvent appréhender différemment les contenus selon leurs valeurs. Dès lors, il faudra tenir compte de la formulation des déclarations, du contexte dans lequel les déclarations ont été faites et les possibles conséquences pour les individus. Ces éléments seront pris en compte de manière subjective selon les États membres. Pour autant, un élément objectif doit être pris en compte dans l'appréciation : lorsque le matériel a été produit par une personne, un groupe, ou une entité figurant sur la liste de l'Union des personnes, groupes et entités impliqués dans des actes terroristes et sujets à des mesures restrictives[322].

[320] *Ibid.*, article 2.7.
[321] *Ibid.*, considérant 11.
[322] *Ibid.*

Ainsi, la définition du contenu terroriste est volontairement large afin de prendre en compte toutes les situations potentiellement problématiques[323]. Lorsqu'un contenu à caractère terroriste est identifié, le règlement impose une procédure d'injonction de retrait dans l'heure[324]. Par-delà la notion de contenu à caractère terroriste, il existe d'autres contenus litigieux présents sur les plateformes : les contenus haineux.

2. Les contenus haineux

94. Définition du contenu haineux. La terminologie « contenu haineux » s'est peu à peu imposée au fil du temps sans faire l'objet d'une définition juridique. Pourtant, dès 1997, le Conseil de l'Europe avait précisé dans une recommandation que « le terme "discours de haine" doit être compris comme couvrant toutes formes d'expression qui propagent, incitent à, promeuvent ou justifient la haine raciale, la xénophobie, l'antisémitisme ou d'autres formes de haine fondées sur l'intolérance, y compris l'intolérance qui s'exprime sous forme de nationalisme agressif et d'ethnocentrisme, de discrimination et d'hostilité à l'encontre des minorités, des immigrés et des personnes issues de l'immigration[325]. ». Il s'agit d'une notion qui s'étend « de manière anarchique, au gré des textes et des enjeux politiques du moment[326]. ».

95. Exercice de proportionnalité. En réalité, la définition du contenu « haineux » constitue un subtil exercice de proportionnalité. Il convient de rechercher un juste équilibre entre la répression sans trop atteindre la liberté d'expression[327]. En effet, « sans définition pertinente de

---

[323] Bertrand Brunessen, « La lutte contre la diffusion des contenus à caractère terroriste en ligne », RTD eur., 2022, 485.

[324] En vertu de l'article 3 du règlement (UE) 2021/784, le destinataire de la présente injonction de retrait retire le contenu à caractère terroriste ou bloque l'accès à ce contenu dans tous les États membres dès que possible et, en tout état de cause, dans un délai d'une heure à compter de la réception de l'injonction de retrait.

[325] Recommandation n° R (97) 20 du Comité des ministres aux états membres sur le « discours de haine », en date du 30 octobre 1997.

[326] Bigot Christophe, « Dispositif actuel de lutte contre la haine en ligne », Pratique du droit de la presse, Dalloz, 2023/2024.

[327] Favro Karine et Zolynski Célia, « De la régulation des contenus haineux à la régulation des contenus (illicites) », Légipresse, 2019, 461 : « Le discours haineux tel qu'il est envisagé, établit une forme d'ordre moral extérieur à l'État et subjectif, qui se révèle d'un maniement liberticide en raison des interprétations possibles et la capacité des plateformes en fonction de leur "poids social" de les retirer promptement. Faire taire ce type de contenus ne permet pas en réalité d'identifier les comportements répréhensibles ou tout simplement à risque, et s'oppose à ce que les utilisateurs soient éduqués à ce type de contenus : la surcensure ne combat pas la haine. ».

ces contenus, sans proportionnalité de la répression et sans prédétermination du bon niveau de régulation, c'est la liberté d'expression qui est en tension[328] ». En 2019, la proposition de la loi « Avia » avait fait le constat d'une prolifération des contenus haineux sur les plateformes, particulièrement les réseaux, et dénonçait l'ambivalence de leurs statuts[329]. La « haine » ne pouvant être réellement définie, la loi s'était contentée d'énumérer des comportements considérés comme haineux[330]. La proposition de loi prévoyait le retrait par les plateformes sous une heure des contenus à caractère terroriste ou pédopornographique notifiés par l'autorité administrative et sous vingt-quatre heures les contenus « manifestement illicites » signalés par tout internaute. Dans une décision du 18 juin 2020, le Conseil constitutionnel a censuré en grande partie la proposition de loi Avia[331]. Le Conseil relève le caractère « louable » de l'objectif poursuivi par la loi tout en censurant pour atteinte disproportionnée à la liberté d'expression. Dans sa décision, le Conseil constitutionnel rappelle qu'il existe un fil rouge à respecter : préserver l'équilibre entre la sauvegarde public et la liberté d'expression[332].

96. Une notion en construction. Le législateur a donc continué ses travaux dans la Loi n° 2021-1109 du 24 août 2021 confortant le respect des principes de la République. Le 28 novembre 2022, en application de l'article 42 de ladite loi, l'ARCOM a publié le 28 novembre 2022 des lignes directrices à destination des opérateurs de plateformes en ligne tenus de contribuer à la lutte contre la diffusion des contenus haineux en ligne[333]. Les lignes directrices visent des contenus relatifs à une « atteinte grave ou imminente à la vie ou à l'intégrité physique, ou qui visent expressément une personne particulièrement vulnérable, dès lors que les opérateurs ont connaissance de la menace et de la qualité de cette personne[334] ». Par ailleurs, le législateur donne la possibilité à toute personne de signaler un contenu haineux. Ainsi,

---

328 Favro Karine et Zolynski Célia, « Penser la régulation à l'ère de la conversation », *Penser le droit de la pensée : Mélanges en l'honneur de Michel Vivant*, éd. Dalloz, 2020, p. 122.

329 Bernard Meyer Hippolyte, « La question de la lutte contre les contenus haineux dans le cyberespace, une réponse nécessairement européenne ? », Revue de l'Union européenne, 2024, p. 29.

330 Letteron Roseline, « La haine sur internet, ou la police exercée par les GAFA », publié sur le blog Liberté, Libertés chéries, 10 juillet 2019.

331 Conseil constitutionnel, décision n° 2020-801 DC du 18 juin 2020 ; Michaël Ghnassia, « Après la censure de la loi contre la haine en ligne, quel avenir pour la répression des contenus haineux sur internet ? », Légipresse, 2020, 419.

332 Mariez Jean-Sébastien et Godfrin Laura, « Censure de la loi "Avia" par le Conseil constitutionnel : un fil rouge pour les législateurs français et européens ? », Dalloz Actualité, 29 juin 2020.

333 Loi n° 2021-1109 du 24 août 2021 confortant le respect des principes de la République.

334 ARCOM, « Lignes directrices prises pour contribuer à la lutte contre la dissémination des contenus haineux en ligne », 2021, p. 3.

l'utilisateur détient la responsabilité de déterminer s'il s'agit d'un contenu haineux ou non. L'appréciation de la notion par l'utilisateur devient alors entièrement subjective.

À l'instar des contenus à caractère terroriste, il sera nécessaire de prendre en compte le contexte et la formulation du contenu. Il ressort de ces définitions que la notion de contenu terroriste est plus encadrée que la notion de contenu haineux. En raison de l'atteinte à la liberté d'expression, la notion de contenu haineux est une notion extrêmement délicate à définir. Pour autant, ces définitions sont désormais intégrées dans une définition générique encore plus extensive : les contenus illicites.

B) Les contenus illicites

97. Définition large et privée. Les contenus illicites font l'objet d'une définition large afin de prendre en compte tous les contenus litigieux (1). En l'absence de définition pendant un certain temps, les plateformes ont encadré cette notion selon leur prisme. La définition du contenu illicite se retrouve privatisée par les géants du numérique (2).

1. La notion large de contenu illicite

98. Définition du contenu illicite. Il était devenu indispensable d'encadrer les contenus illicites dont le volume est impressionnant : « l'objectif est infiniment louable, mais la tâche à accomplir est démesurée[335] ». La difficulté résulte dans la mission d'établir une définition large tout en étant assez précise afin de pouvoir responsabiliser les acteurs concernés[336]. Également, il est nécessaire de prendre en compte l'humour, l'ironie ou les logiques de contre-discours qui viennent irriguer certains contenus[337]. Le Règlement (UE) 2022/2065 du 19 octobre 2022 du Parlement européen et du Conseil relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (DSA) retient une définition large.

[335] Mallet-Poujol Nathalie, « Plateformes en ligne et modération des contenus : la liberté d'expression à l'épreuve du concept d'évidence », Légipresse, 2024, 348.
[336] Favro Karine et Zolynski Célia, « Penser la régulation à l'ère de la conversation » in Geiger Christophe (dir.), Penser le droit de la pensée : Mélanges en l'honneur de Michel Vivant, éd. Dalloz, 2020, p. 122.
[337] Mallet-Poujol Nathalie, « Plateformes en ligne et modération des contenus : la liberté d'expression à l'épreuve du concept d'évidence », Légipresse, 2024, 348.

99. Définition par exclusion. La définition du contenu illicite est imprégnée du discours selon lequel « tout ce qui est interdit hors ligne doit l'être en ligne[338] ». En effet, le considérant 12 du règlement précise que la notion doit correspondre de manière générale aux règles en vigueur dans l'environnement hors ligne[339]. La notion doit être comprise « comme se référant à des informations, quelle que soit leur forme, qui, en vertu du droit applicable, sont soit elles-mêmes illicites, comme les discours haineux illégaux ou les contenus à caractère terroriste et les contenus discriminatoires illégaux, soit rendues illicites par les règles applicables en raison du fait qu'elles se rapportent à des activités illégales[340] ». D'une manière cohérente, les contenus haineux et terroristes sont compris dans la définition. Le considérant précité précise qu'il peut s'agir : « du partage d'images représentant des abus sexuels commis sur des enfants, du partage illégal d'images privées sans consentement, du harcèlement en ligne, de la vente de produits non conformes ou contrefaits, de la vente de produits ou de la fourniture de services en violation du droit en matière de protection des consommateurs, de l'utilisation non autorisée de matériel protégé par le droit d'auteur, de l'offre illégale de services de logement ou de la vente illégale d'animaux vivants recouvrant les informations relatives aux contenus, produits, services et activités illicites[341] ». En réalité, la notion de contenu illicite a pendant longtemps été privatisée par les protagonistes de la diffusion des contenus sur l'environnement numérique : les géants du numérique.

2. La privatisation de la notion du contenu illicite

100. Définition du contenu illicite par les plateformes. L'absence de définition avant l'entrée en vigueur du règlement sur les services numériques a permis aux plateformes de dégager les contours de la notion dans leurs conditions générales. Pendant longtemps, les plateformes ont adopté des « politiques de modération "maison" fondées sur leurs propres standards[342] ». En effet, depuis quelques années, les plateformes régissent les contenus disponibles sur leurs plateformes dans leurs conditions générales. D'une façon mythique, les utilisateurs d'une plateforme constitueraient une « communauté » : les réseaux seraient d'une

[338] Le Commissaire européen Thierry Breton s'était exprimé en ce sens : « Tout ce qui est interdit hors ligne doit l'être en ligne. ».
[339] Règlement (UE) 2022/2065 du 19 octobre 2022 du Parlement européen et du Conseil relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (règlement sur les services numériques), considérant 12.
[340] *Ibid.*
[341] *Ibid*.
[342] Meta, « Modalités d'application de nos politiques relatives au contenu », espace modération, août 2023.

nature philanthropique et auraient pour dessein de protéger leurs utilisateurs. Il s'agit de l'histoire que les géants du numérique aiment conter aux nouveaux utilisateurs. Afin d'évoluer dans un environnement sain et participatif, les internautes doivent respecter les « standards de la communauté », notifiés dans les conditions générales.

À titre d'illustration, Meta explique ne pas autoriser les contenus qui incitent à la violence et aux comportements criminels (comme les contenus qui promeuvent les organisations dangereuses, leur viennent en aide ou en font l'éloge), qui compromettent la sécurité des personnes (comme l'intimidation et le harcèlement, le suicide et l'automutilation, et l'exploitation sexuelle d'enfants ou d'adultes), qui sont répréhensibles (comme les discours haineux), qui ne sont pas authentiques (comme les spams, les fausses informations ou les faux profils) ou qui violent les droits de propriété intellectuelle d'autrui. D'autres contenus ne sont pas autorisés car moralement réprouvés et préjudiciables pour une partie de la population, comme la nudité[343] . En réalité, ces actions philanthropiques de Facebook sont simplement une utopie.

101. Privatisation de la modération. Pour autant, l'article 34 du Règlement (UE) 2022/2065 du 19 octobre 2022 du Parlement européen et du Conseil relatif à un marché unique des services numériques reprend cette pratique et vise comme objet de modération les « contenus illicites » mais également les « informations incompatibles avec leurs conditions générales »[344]. Les géants du numérique peuvent donc mettre en place un instrument d'autorégulation pour les contenus qu'ils jugent illicites. Il n'est pas certain que la balance entre répression et liberté d'expression soit assurée. D'un côté, le législateur accepte une définition large afin de prendre en compte les évolutions de la société. De l'autre, le législateur intègre un réel pouvoir d'autocensure de la part de sociétés privées, non légitimes. Il n'est pas certain que les plateformes agissent dans un but altruiste et cherchent à combattre les contenus illicites.

[343] Cluzel-Métayer Lucie, « Contrôler les contenus ? », Pouvoirs, 185, Le Seuil, 2023.

[344] Mallet-Poujol Nathalie, « Plateformes en ligne et modération des contenus : la liberté d'expression à l'épreuve du concept d'évidence », Légipresse, 2024, 348 : « À l'égard de tels contenus, parfois qualifiés de "crus", l'opérateur de la plateforme, drapé sous la bannière de la "communauté" exerce une police de l'expression, au nom d'une forme de bienséance, pour assurer le bien-être et la sécurité de ses membres. Le bien-fondé de la démarche d'autorégulation est indéniable. Reste à savoir, au plan juridique, s'il est possible, dans toutes les hypothèses, d'imposer à l'usager du service de renoncer au plein exercice de la liberté d'expression en acceptant de s'autocensurer sur la publication de certains propos ou de certaines images. ».

102. Manipulation de la modération. En effet, les géants du numérique se rémunèrent en grande partie avec la publicité ciblée dépendante du temps passé par les utilisateurs sur leur plateforme. Le temps est manipulé par des contenus engageants et généralement à la limite de l'illicéité[345]. Ils peuvent alors être tentés de choisir de laisser en ligne un contenu polémique ou violent pour des raisons commerciales[346]. Pire encore, ils développent des techniques subreptices de manipulation et d'ordonnancement des contenus. Ainsi, il est permis de douter que les conditions générales d'utilisation de ces plateformes soient conformes aux valeurs européennes. Au contraire, ils se servent de la liberté d'expression afin d'exercer un contrôle des contenus à leur profit pour préserver leurs intérêts économiques. Le pouvoir accordé à ces plateformes peut être qualifié de « privatisation de la liberté d'expression[347] ». Fort heureusement, cette pratique est sans préjudice pour les utilisateurs d'engager à tout moment, une procédure pour contester lesdites décisions prises par les fournisseurs de plateformes en ligne devant une juridiction[348].

103. Intelligence artificielle générative. Par ailleurs, le développement des intelligences artificielles génératives réamorce le débat sur les contenus illicites. L'intelligence artificielle générative est une branche de l'intelligence artificielle mettant en œuvre des modèles génératifs, visant à produire des contenus textuels, graphiques ou audiovisuels[349]. Cette branche de l'intelligence artificielle pourrait générer et diffuser des contenus illicites sur les plateformes. En effet, les plateformes vont utiliser ces technologies afin de partager du contenu à leurs utilisateurs dans le dessein d'accentuer les conflits, de distraire les internautes ou de leur faire passer toujours plus de temps sur leur téléphone[350]. Néanmoins, cette technologie peut servir de

[345] Comme l'a démontré la lanceuse d'alerte Frances Haugen.
[346] Cluzel-Métayer Lucie, *op. cit*., p. 117.
[347] Iliopoulou-Penot Anastasia, « La Constitution numérique européenne », RFDA, 2023, 945 .
[348] Règlement (UE) 2022/2065 du 19 octobre 2022 du Parlement européen et du Conseil relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (règlement sur les services numériques), considérant 59 : « Les destinataires du service devraient pouvoir choisir entre le mécanisme interne de traitement des réclamations, un règlement extrajudiciaire des litiges et la possibilité d'engager, à tout moment, une procédure juridictionnelle. Étant donné que l'issue de la procédure de règlement extrajudiciaire des litiges n'est pas contraignante, les parties ne devraient pas être empêchées d'engager une procédure judiciaire concernant le même litige. ».
[349] Journal Officiel de la République Française (JORF), n° 0212, v° « intelligence artificielle générative », 6 septembre 2024.
[350] Coglianese Cary, « Regulating Machine Learning : The Challenge of Heterogeneity », Competition Policy International : TechReg Chronicle, 2023, Public Law Research Paper.

« super propagateur d'infox[351] ». Selon les auteurs de cet article, dans 80% des cas, ChatGPT a relayé des informations trompeuses sur les sujets d'actualité comme la Covid-19, l'Ukraine et les fusillades dans les écoles aux États-Unis. Ainsi, le débat dépasse les utilisateurs et la responsabilité des plateformes.

[351] Brewster Jack, Arvanitis Lorenzo et Sadeghi McKenzie, « Le prochain super propagateur d'infox », sur NewsGuard, 2023.

104. Conclusion de la section. Il ressort de l'analyse de la notion de « contenu » que les données constituent la matière première des contenus. À l'instar des données, la nature des contenus est polymorphe : il peut s'agir d'informations personnelles d'un internaute, d'informations relatives à un historique de navigation ou encore de contenus publiés volontairement. Les contenus numériques peuvent également se présenter sous forme de services. Les notions de « données » et d' « informations » s'intègrent donc dans la notion de contenu.

Les contenus sont des données interprétées, à forte valeur ajoutée. En pratique, les contenus représentent un intérêt économique majeur pour les plateformes et les acteurs du numérique profitent de la surproduction de contenus afin de faire valoir leurs propres intérêts économiques. Grâce à leurs algorithmes, les plateformes proposent des contenus toujours plus personnalisés en fonction des informations récoltées afin de maintenir l'attention des utilisateurs sur leur plateforme. Ensuite, les plateformes se rémunèrent par la publicité ciblée et l'exploitation des données à caractère personnel des utilisateurs. Ainsi, les contenus représentent une réelle source de valeur pour les plateformes grâce à la publicité ciblée. Les données sur la réception d'un contenu par les utilisateurs sont également une source de valeur pour les plateformes qui peuvent sans cesse améliorer les contenus disponibles ainsi que leurs services.

Néanmoins, il existe également une part de contenus illicites diffusés sur les plateformes. Il peut s'agir de contenus pédopornographiques, à caractère terroriste ou encore des contenus haineux. La diffusion des contenus illicites représente un risque pour les utilisateurs et pour la société. Le législateur entreprend donc des travaux de définition des contenus illicites. La tâche est hasardeuse tant il est difficile de trouver une définition suffisamment répressive tout en respectant la liberté d'expression.

En réalité, les plateformes deviennent de plus en plus responsables des contenus au gré des législations. Pour autant, les plateformes ne sont pas motivées par des objectifs d'intérêt général. Les contenus engageants - souvent illicites - sont les contenus qui provoquent le plus d'engagement. Il est légitime de penser que les plateformes vont parfois effectuer des choix mercantiles et non altruistes pour la suppression d'un contenu.

105. Conclusion du chapitre. Les notions de « donnée », d'« information » et de « contenu » sont intiment liées. En effet, l'information est une donnée interprétée et mise en contexte. L'information est ensuite intégrée dans un contenu, représentant la matière première. La valeur du contenu est donc directement liée aux données. Plus les données sont traitées, exploitées et raffinées, plus le contenu sera pertinent. Avec l'aide des algorithmes, les plateformes développent et diffusent des contenus personnalisés pour les internautes. Lorsque les contenus sont personnalisés, les plateformes captent l'attention de l'utilisateur. La maîtrise des contenus par les plateformes représente la plus grande partie de leurs bénéfices, à travers la publicité ciblée.

Ainsi, par-delà la valeur propre de ces notions, c'est donc la valeur d'usage qui est fondamentale. Les plateformes collectent les données, transforment les données en informations, utilisent ces informations afin de créer de nouveaux produits, d'améliorer leurs algorithmes, et de diffuser des contenus et services personnalisés aux utilisateurs. La maîtrise de l'attention des internautes permet aux plateformes d'ordonnancer les contenus. L'ordonnancement s'effectue selon les contenus à fort engagement, c'est-à-dire les contenus provocateurs, voire illicites.

Le rôle des plateformes n'est pas neutre et ils profitent - sous couvert de la liberté d'expression - de la maîtrise de leur environnement pour entraîner leurs algorithmes. L'unique dessein de ces entreprises privées est de faire augmenter les bénéfices. En réalité, ils captent les données à caractère personnel des utilisateurs afin de leur proposer des contenus adaptés selon les informations déduites de leurs données.

Afin de prendre en compte cette réalité, le législateur a saisi les données comme nouvel objet de droit et entreprend le délicat travail de définition, étape préalable de l'application du régime juridique.

Chapitre 2 :

La notion juridique de données : forces et faiblesses

106. Diverses définitions. Au regard de la nature polymorphe des notions, les données et les informations ne peuvent faire l'objet d'un unique qualificatif. La donnée peut être qualifiée de brute, personnelle, non personnelle, publique, privée. Avec l'usage exponentiel des données, le droit a saisi les données comme objet de droit, en établissant différentes catégories de données.

Au fil du temps, de nouvelles catégories de données apparaissent afin de prendre en compte les nouveaux usages. En fonction de sa nature, de la personne dont elle émane ou de son potentiel, chaque donnée fait l'objet d'une définition propre. La notion juridique de la donnée est donc dépendante de la typologie des données (**Section 1**), typologie qui se révèle instable en considération de l'usage des technologies émergentes (**Section 2**).

Section 1 : L'instauration d'une typologie des données

107. Catégorie de données. Les principales catégories de données sont les données à caractère personnel et les données à caractère non personnel (I). Il existe également une large catégorie pour les données publiques, qui peuvent être à caractère personnel ou non (II).

I. Les notions de données à caractère personnel et données à caractère non personnel

108. Nouvelles catégories de données. Les notions de données à caractère personnel et non personnel font partie d'une catégorie générale des données (A). Néanmoins, les nouveaux usages ont fait émerger de nouvelles catégories de données, intégrées ou non par le droit (B).

A) Les définitions des données à caractère personnel et non personnel

109. Définition large ou par défaut. Afin de prendre en compte l'essor des technologies émergentes d'identification, le droit dérivé a retenu une définition large de la donnée à caractère personnel (1), tandis que la donnée à caractère non personnel fait l'objet d'une définition par défaut (2).

1. Définition large de la donnée à caractère personnel

110. Définition légale. La notion de « données à caractère personnel » est définie, par l'article 4.1 du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (RGPD) comme suit « toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée "personne concernée") ; est réputée être une "personne physique identifiable" une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale[352] ». La définition est reprise par l'article 2 de la Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, entrée en vigueur dans sa nouvelle version le 1er juin 2019[353]. La définition est une notion générique applicable à tous les secteurs d'activité, favorisant l'émergence d'une notion souple[354].

111. Approche restrictive. La notion de données à caractère personnel a été substituée par la loi du 6 août 2004 à la notion « d'informations nominatives »[355]. La notion d'informations nominatives ne visait que les éléments d'identification en relation avec le nom de la personne. Par cette approche, la notion était restrictive[356]. Or, avec le développement des progrès techniques d'identification, la notion ne prenait pas en compte les techniques d'identification indirecte[357]. Désormais, la notion de données à caractère personnel vise « toute information » à

[352] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).
[353] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, article 2, alinéa 2 : « Constitue un fichier de données à caractère personnel tout ensemble structuré de données à caractère personnel accessibles selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique. ».
[354] Vergnolle Suzanne, *L'effectivité de la protection des personnes par le droit des données à caractère personnel,* éd. Larcier, 2022, p. 125.
[355] 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 ; Lesaulnier Frédérique, « L'information nominative », Thèse, Paris, 2005.
[356] Douville Thibault, *Droit des données à caractère personnel*, éd. LGDJ, 2023, p. 99.
[357] Eynard Jessica, *Les données personnelles. Quelle définition pour un régime de protection efficace ?*, éd. Michalon, 2013, p. 31.

propos d'une personne physique. Il peut s'agir du nom, du prénom, du numéro de téléphone, de la date de naissance : peu importe la nature de l'information à partir du moment où la personne peut être identifiée ou identifiable. L'information doit simplement se rapporter à une personne physique[358]. En effet, la notion comporte tout type d'informations : informations privées, publiques, professionnelles ou commerciales, informations objectives ou subjectives[359]. Il suffit que la donnée porte sur des personnes physiques, « vivantes, identifiées, ou identifiables ».

112. Définition extensive. De surcroît, la notion de données à caractère personnel apparaît plus pertinente en ce qu'elle permet de couvrir des informations permettant l'identification, tant directe mais également indirecte que de la personne[360]. L'identification de la personne physique peut se faire de manière directe, par exemple en utilisant le nom et le prénom de la personne, et de manière indirecte, par exemple avec un numéro de téléphone, une plaque d'immatriculation, une adresse postale, la voix ou l'image. L'identification peut également se faire à partir d'une seule donnée, par exemple le nom, ou à partir du croisement de plusieurs données, par exemple avec l'adresse et la date de naissance. La personne physique peut être identifiable lorsqu'on regroupe plusieurs informations, sans nécessairement connaître son identité. La notion de données à caractère personnel regroupe des données de toute nature, telles que les données biométriques, des informations de localisation ou encore des traces diverses qui peuvent identifier une personne grâce aux corrélations. Ainsi, sont des données à caractère personnel l'empreinte digitale, la localisation opérée par GPS, un pseudonyme ou encore les goûts et opinions[361].

---

358 Tribunal de l'Union européenne, aff. T-557/20, Conseil de résolution unique (CRU) c/ Contrôleur européen de la protection des données (CEPD), 26 avril 2023, point 68 sur l'interprétation large de la notion qui ne doit pas être « restreinte aux informations sensibles ou d'ordre privé, mais englobe potentiellement toute sorte d'informations, tant objectives que subjectives sous forme d'avis ou d'appréciations, à condition que celles-ci "concernent" la personne en cause ».

359 De Terwangne Cécile et Rosier Karen, *Le règlement général sur la protection des données. Analyse approfondie,* éd. Larcier, 2018, p. 60.

360 Benabou Valérie-Laure, « L'extension du domaine de la donnée », Legicom, n° 59, Victoires éditions, 2017.

361 Eynard Jessica, « Identité, données d'identification personnelle, données personnelles », *in* Eynard Jessica (dir.), *L'identité numérique*, éd. Larcier, 2020, p. 97.

À titre d'illustration, la Cour de cassation a opéré un revirement de jurisprudence le 3 novembre 2016, suite à la position de la Cour de justice de l'Union européenne, en reconnaissant explicitement que les adresses IP, qui permettent d'identifier indirectement une personne physique, sont des données à caractère personnel[362]. Techniquement, les adresses IP (Internet Protocol) ne sont pas liées à une personne physique mais à une machine. Pourtant, pour la Cour de justice de l'Union européenne, « le fait qu'il existe des voies légales permettant à l'exploitant d'un site de s'adresser aux autorités pour que celles-ci entreprennent les démarches nécessaires afin d'obtenir ces informations auprès du fournisseur d'accès à Internet, suffit à qualifier de "données à caractère personnel" les adresses IP » [363]. La jurisprudence approuve la même position pour les adresses MAC (*Media Access Control*)[364].

113. Indifférence des éléments. Avec cette définition, la notion de donnée à caractère personnel est devenue une notion extensive permettant de prendre en compte l'ensemble des d'informations sur une personne physique[365]. De surcroît, avec les traces laissées par les individus sur Internet, leur combinaison permet de créer des profils de personnes physiques et d'identifier ces personnes[366]. Afin de prendre en compte les évolutions des techniques d'identification, cette nouvelle notion est indifférente de la technologie employée pour accéder à l'identification des individus et appréhende de nouveaux outils ayant cette aptitude (*cookies*, objets connectés, etc.)[367]. Par cette indifférence, une très grande proportion des données collectées par des technologies numériques constitue des données à caractère personnel. Par ailleurs, la véracité ou l'exactitude des informations n'a aucune incidence sur la qualification des données à caractère personnel[368]. Ainsi, dès lors qu'une information permet d'identifier de

362 Cour de cassation, Chambre civile 1, 3 novembre 2016, 15-22.595, publié au bulletin.

363 L'adresse IP (« IP » pour Internet Protocol) correspond au numéro identifiant une interface technique (un ordinateur, une imprimante, un routeur, etc) connectée avec le réseau Internet. Une adresse IP peut être « fixe (auquel cas, elle sera toujours la même lorsqu'un terminal - un ordinateur, par exemple - se connectera à Internet) ou bien « dynamique » (l'utilisateur se verra attribuer une nouvelle adresse IP par son fournisseur d'accès à Internet, à chaque connexion). Définition reprise par la Cour de justice de l'Union européenne dans son arrêt du 19 octobre 2016 (aff. C-582/14, point 36).

364 Une adresse MAC est l'adresse physique d'une carte réseau permettant d'identifier de façon unique un équipement sur le réseau local (CNIL, délibération, n°2016-053, 1er mars 2016)

365 Benabou Valérie-Laure, « L'extension du domaine de la donnée », Legicom, n° 59, 2017.

366 Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), considérant 30.

367 Benabou Valérie-Laure, *op. cit*.

368 Douville Thibault, *op. cit*., p. 104.

manière directe ou indirecte une personne physique, elle est considérée donc comme une donnée à caractère personnel et, est soumise au régime de la Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, régime renforcé par le RGPD.

Pour autant, toutes les données ne sont pas des données à caractère personnel : il existe également un grand nombre de données à caractère non personnel, faisant l'objet d'une définition par opposition aux données à caractère personnel.

2. Définition par opposition de la donnée à caractère non personnel

114. Définition légale. La notion de donnée à caractère non personnel est une définition par opposition aux données à caractère personnel[369]. Le Règlement (UE) 2018/1807 du Parlement européen et du Conseil du 14 novembre 2018 établissant un cadre applicable au libre flux des données à caractère non personnel dans l'Union européenne définit la donnée à caractère non personnel au sein de son article 3 comme toutes « les données autres que les données à caractère personnel au sens de l'article 4, point 1), du règlement (UE) 2016/679 ». De ce fait, le règlement instaure une dichotomie entre les données à caractère personnel et les données à caractère non personnel. Selon cette conception, le législateur renverse le point de départ de la qualification : par principe, les données sont en lien avec une personne physique[370].

En pratique, les données à caractère non personnel se distinguent selon leur origine en deux catégories : les données qui, au départ, ne concernaient pas une personne physique identifiée ou identifiable et, les données qui étaient initialement des données à caractère personnel, mais qui ont ensuite été rendues anonymes[371]. Si tel n'est pas le cas, le règlement précise que si les évolutions technologiques permettent de transformer les données anonymisées en données à caractère personnel, ces données doivent être traitées comme des données à caractère personnel et le règlement 2016/279 du 17 avril 2016 doit s'appliquer en conséquence.

369 Nevejans Nathalie, *op. cit*., p.17.
370 Vergnolle Suzanne, *L'effectivité de la protection des personnes par le droit des données à caractère personnel,* éd. Larcier, 2022, p. 119.
371 Commission européenne, « Lignes directrices relatives au règlement concernant un cadre applicable au libre flux des données à caractère non personnel dans l'Union européenne », COM (2019) 250 final, p. 6.

115. Diversité des données à caractère non personnel. Le considérant 9 du Règlement (UE) 2018/1807 du Parlement européen et du Conseil du 14 novembre 2018 établissant un cadre applicable au libre flux des données à caractère non personnel dans l'Union européenne précise que « l'essor de l'Internet des objets, l'intelligence artificielle et l'apprentissage automatique représentent des sources importantes de données à caractère non personnel ». Ces données représentent un intérêt stratégique pour le développement du marché unique numérique. Ainsi, la définition des données à caractère non personnel « permet de saisir en droit la donnée produite en masse par des machines connectées produisant des données captées et stockées chez des prestataires de services, des procédés fondés sur des technologies émergentes comme l'Internet des objets ou les systèmes connectés autonomes[372] ». Il peut s'agir de données sur l'agriculture de précision qui peuvent aider à contrôler et à optimiser l'utilisation des pesticides et de l'eau, ou encore les données sur les besoins d'entretien des machines industrielles[373].

116. Champ des données à caractère non personnel. Le champ des données à caractère non personnel est extrêmement large et contient des données dépersonnalisées, certaines données publiques et des données privées. Les données dépersonnalisées sont des données qui n'ont pas fait l'objet d'un traitement au sens de l'article 3 du règlement, entendant le traitement au sens large du terme, c'est-à-dire quel que soit le système informatique utilisé. Les données privées sont les données qui sont produites par les entreprises. Pour inciter les entreprises à libérer leurs données, la Commission précise que le principe de proportionnalité doit être mis en œuvre afin de concilier les intérêts des entreprises et les finalités de libre circulation. Quant aux données publiques, le champ de la donnée non personnelle absorbe en grande partie celui de la donnée publique[374].

Par-delà la dichotomie entre données à caractère personnel et données à caractère non personnel, il existe des catégories particulières de données.

[372] *Ibid.*, p. 35.
[373] Règlement (UE) 2018/1807 du Parlement européen et du Conseil du 14 novembre 2018 établissant un cadre applicable au libre flux des données à caractère non personnel dans l'Union européenne, considérant 9.
[374] Favro Karine, « "Les données non personnelles" : un nouvel objet juridique », Dalloz IP/IT, 2020.

B) Les catégories particulières de données

117. Les catégories spécifiques de données. Au sein de la catégorie des données à caractère personnel, des règles spécifiques sont régies afin de prendre en compte des données dites « sensibles » (1). De surcroît, le développement des technologies émergentes fait apparaître de nouvelles notions de données (2).

1. Les données sensibles

118. Nature des données sensibles. Les données sensibles forment une catégorie particulière des données à caractère personnel en raison de leur nature. Il existe des données directement sensibles par nature et des données indirectement sensibles dans la mesure où elles révèlent des informations jugées sensibles. À titre d'illustration, une donnée génétique est sensible par nature et une donnée sur l'opinion politique est sensible du fait de l'information révélée[375]. La nature de ces données représente des enjeux particulièrement sensibles en matière de risques pour les droits et libertés des personnes concernées[376]. La Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés énonce un principe d'interdiction de traitements des informations qui révèlent la prétendue origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale et les données de santé[377]. *In fine*, le degré de protection concernant la nature des données se fait « plus faible s'agissant des couches extérieures, elle se fait plus ferme lorsque s'agissant des couches de données les plus intimes[378] ».

119. Données génétiques et biométriques. Conformément au Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, la loi Informatique et Libertés a étendu les données sensibles aux données

---

375 Charpentier Arthur, Cocteau-Senn Delphine, Bigot Rodolphe, « La protection des données personnelles en assurance : dialogue du juriste avec l'actuaire », *in* Netter Emmanuel, *Regards sur le nouveau droit des données personnelles*, éd. CEPRISCA, 2019, p. 259.

376 Martial-Braz Nathalie et Rochfeld Judith, *Droit des données personnelles. Les spécificités du droit français au regard du RGPD*, éd. Dalloz, 2019, p. 91 ; Christina Koumpli, « Les données personnelles sensibles : contribution à l'évolution du droit fondamental à la protection des données personnelles : étude comparée : Union Européenne, Allemagne, France, Grèce, Royaume-Uni », Thèse, Paris, 2019.

377 Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, article 8.

378 Netter Emmanuel, *Numérique et grandes notions de droit privé*, éd. CEPRISCA, 2019, p. 97.

génétiques et biométriques, ainsi qu'aux données relatives à l'orientation sexuelle d'une personne. Les données génétiques étant définies comme « des données à caractère personnel relatives aux caractéristiques génétiques héréditaires d'une personne qui donnent des informations uniques sur la physiologie ou l'état de santé de cette personne et qui résultent, notamment, d'une analyse d'un échantillon biologique de la personne physique en question[379] » et les données biométriques comme « des données à caractère personnel résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique, qui permet une identification unique, telles que des images faciales ou des données dactyloscopiques[380] ». De surcroît, toujours au sein de la catégorie des données sensibles, la notion de donnée de santé a été révisée.

120. La donnée de santé, une donnée particulièrement sensible. Les données de santé sont des données à caractère personnel particulières, considérées comme des données sensibles. Les données de santé sont soumises à un régime particulier au regard de leur nature. Pour autant, la donnée de santé ne faisait pas l'objet d'une définition au sein de la 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. En 2004, la notion va être intégrée dans la 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, sans pour autant en donner une véritable définition textuelle[381]. Néanmoins, la CJCE avait rappelé dès 2003 qu'il convient de donner à l'expression « données relatives à la santé » employée à son article 8, paragraphe 1er, une « interprétation large de sorte qu'elle comprenne des informations concernant tous les aspects, tant physiques que psychiques, de la santé d'une personne[382] ».

121. Définition légale des données de santé. Depuis l'entrée en vigueur du RGPD, les données de santé sont définies à l'article 4, alinéa 15 comme des données « relatives à la santé

[379] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), article 4, point 13.
[380] *Ibid*., article 4, point 14.
[381] 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.
[382] Cour de Justice des communautés européennes (CJCE), aff. C-101, « Bodil Lindqvist », 6 novembre 2003.

physique ou mentale d'une personne physique, y compris la prestation de service de soins de santé, qui révèlent des informations sur l'état de santé de cette personne ». Le considérant 35 précise l'étendue de la nouvelle définition. Il souligne tout d'abord l'absence d'ancrage temporel des données de santé qui peuvent se rapporter à l'état de santé passé, présent ou futur d'une personne[383] . Surtout, la définition fait référence à une personne physique et non à un patient, permettant d'élargir la notion.

Ensuite, le présent considérant donne une liste d'exemples de données pouvant entrer dans la catégorie des données de santé comme « des informations sur la personne physique collectées lors de l'inscription de cette personne physique en vue de bénéficier de services de soins de santé ou lors de la prestation de ces services au sens de la directive 2011/24/UE du Parlement européen et du Conseil au bénéfice de cette personne physique ; un numéro, un symbole ou un élément spécifique attribué à une personne physique pour l'identifier de manière unique à des fins de santé ; des informations obtenues lors du test ou de l'examen d'une partie du corps ou d'une substance corporelle, y compris à partir de données génétiques et d'échantillons biologiques ; et toute information concernant, par exemple, une maladie, un handicap, un risque de maladie, les antécédents médicaux, un traitement clinique ou l'état physiologique ou biomédical de la personne concernée, indépendamment de sa source, qu'elle provienne par exemple d'un médecin ou d'un autre professionnel de la santé, d'un hôpital, d'un dispositif médical ou d'un test de diagnostic *in vitro*. ».

122. Définition large. Désormais, la notion de donnée de santé est une définition large, faisant une appréciation *in concreto*. La notion intègre tous les éléments nécessaires à la prise en charge sanitaire de la personne, quelle que soit la source de l'information. Pour la Commission nationale de l'informatique et des libertés, trois catégories de données peuvent entrer dans cette notion comme : les données de santé par nature (antécédents médicaux, maladies, résultats d'examens, traitements, handicap, etc), les données croisées avec d'autres données qui deviennent des données de santé en permettant de déterminer l'état de santé d'une personne (croisement d'une mesure de poids avec d'autres données, croisement de la tension avec la mesure de l'effort, etc) ou encore les données qui deviennent des données de santé en raison de

[383] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), considérant 35.

leur destination, soit en raison de l'usage[384]. Par exemple, un usage dans un contexte médical va permettre de qualifier une donnée en donnée de santé. L'intégration de l'usage dans la qualification est une évolution nécessaire et louable.

123. Le Numéro d'Inscription au Répertoire (NIR) : une donnée singulièrement sensible. Définitivement, la catégorie des données sensibles est extensive puisqu'elle intègre également le numéro d'inscription au répertoire national d'identification, le NIR. Ce numéro, communément appelé numéro de sécurité sociale, permet d'identifier les personnes physiques. Il est composé de treize chiffres et d'une clé de contrôle de deux chiffres. Dans ses conclusions sur l'utilisation du NIR, la Commission nationale de l'informatique et des libertés précise qu'il s'agit d'un numéro particulier dans la mesure où il est « signifiant », puisqu'« il est composé d'une chaine de caractères qui permettent de déterminer le sexe, le mois et l'année de naissance, et dans la majorité des cas, le département et la commune de naissance en France ou l'indication d'une naissance à l'étranger, il est unique et pérenne : un seul numéro est attribué à chaque individu dès sa naissance et *a priori* fiable : il est certifié par l'Institut National de la Statistique et des Etudes Economiques (INSEE), à partir des données d'état civil transmises par les mairies[385] ». Ainsi, dans la mesure où le NIR permet d'identifier une personne physique, cela devient une donnée à caractère personnel, extrêmement sensible, dont l'utilisation est très encadrée[386].

En parallèle des catégories précitées de données, de nouvelles notions apparaissent par les nouveaux usages des données.

---

384 Commission nationale de l'informatique et des libertés, « Qu'est-ce ce qu'une donnée de santé ? », disponible en ligne.

385 Commission nationale de l'informatique et des libertés, « Informatique et libertés », Guide, édition 2010, p. 12.

386 Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), article 4, 1 : « "données à caractère personnel", toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée "personne concernée") ; est réputée être une "personne physique identifiable" une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale. ».

2. Les notions de données novatrices

124. Les données de bien-être. Le développement des objets connectés - et particulièrement des capteurs corporels connectés - a fait apparaître une nouvelle notion de données dites « données de bien-être ». Les données se développent dans un mouvement de *quantified self*, autrement dit « d'auto-mesure » ou de « quantification de soi »[387]. Pour la Commission nationale de l'informatique et des libertés, le corps serait devenu un nouvel objet connecté, un nouveau « territoire de la mise en données du monde[388] ». En effet, les objets connectés permettent aux individus de mesurer leurs activités quotidiennes à partir de leurs propres données. Il s'agit par exemple de mesurer son rythme cardiaque, son nombre de pas, son temps de sommeil, ou même de mesurer son humeur. Allant toujours plus loin, les lentilles de contact à réalité augmentée pour le sport ou des vêtements munis de capteurs se développent[389]. Les objets connectés sont généralement reliés à des applications sur les *smartphones* et permettent d'établir des paliers à atteindre afin de réaliser des objectifs déterminés. Par exemple, l'application « *Garmin Connect* » permet de retrouver les données générées par la montre connectée sur son *smartphone* afin d'analyser nos propres données sportives. Les données sont ensuite mesurées, analysées, ou encore être partagées.

125. Confusion avec les données de santé. La nouvelle catégorie de données soulève des incertitudes quant à leur nature puisque si celles-ci relèvent à priori du « bien être », elles peuvent parfois révéler l'état de santé d'un individu et devenir par conséquent des données de santé, c'est-à-dire des données sensibles. En pratique, il existe une confusion entre les données

[387] Andrieu Bernard, « Traquer son bien-être et propriété des données : quel droit des sportifs 3.0 sur leur corps vivant ? », JS, 2016, n°162, p. 36.

[388] Commission nationale de l'informatique et des libertés, « Le corps, nouvel objet connecté. Du quantified self à la M-Santé : les nouveaux territoires de la mise en données du monde », Cahiers IP, n° 02, mai 2014, p. 3 : « Sous cette expression quelque peu sibylline, sont visées des pratiques variées mais qui ont toutes pour point commun pour leurs adeptes, de mesurer et de comparer avec d'autres des variables relatives à notre mode de vie : nutrition, exercice physique, sommeil, mais aussi pourquoi pas son humeur, etc. Reposant de plus en plus sur l'utilisation de capteurs corporels connectés - bracelets, podomètres, balances, tensiomètres, etc. - et d'applications sur mobiles, ces pratiques volontaires d'auto-quantification se caractérisent par des modes de capture des données de plus en plus automatisés, et par le partage et la circulation de volumes considérables de données personnelles. ».

[389] Beguin-Faynel Céline, « Objets connectés et appréciation du risque », Responsabilité civile et assurances, n° 3, mars 2023, dossier 10.

de santé et les données de bien-être : les deux notions sont assurément proches, puisque l'état de santé va permettre de concourir à un certain bien être, et inversement. *In fine*, les données de bien être ne seraient qu'une émanation des données de santé[390]. À ce sujet, l'association française des correspondants à la protection des données à caractère personnel (AFCDP) estime de manière raisonnable que les données de bien être devraient être considérées comme des données de santé dans la mesure où ces données permettent de déduire des conclusions sur l'état de santé ou les risques de la santé d'un individu[391]. En effet, avec le développement des données massives et des technologies d'analyse, les frontières entre les données de bien-être et de santé sont extrêmement poreuses.

126. Privatisation des données de bien-être. Malheureusement, la donnée de bien-être ne recouvre pour l'instant aucune réalité juridique[392]. La notion sème le doute quant à la véritable nature juridique des informations collectées, entre données à caractère personnel et données sensibles pouvant être relatives à la santé[393]. En pratique, l'incertitude juridique permet aux applications de ne pas être soumises au régime contraignant s'appliquant aux données de santé. Cette incertitude est préjudiciable aux utilisateurs dans la mesure où les technologies permettent désormais une interconnexion de ces données : une donnée en apparence non sensible pourra le devenir avec le croisement d'autres données. La collecte de ces données par des « tiers intéressés » s'avère dangereuse à l'ère du *Big Data* : il existe un risque de « privatisation de la santé[394] ». À nouveau, les géants du numérique présentent cette collecte dans un but d'améliorer et de personnaliser les services. En réalité, cette incertitude juridique leur profite et surtout, leur permet de capter les données de bien être des individus afin de les exploiter et de les commercialiser. Les données de bien être deviennent extrêmement sensibles selon l'usage fait par ces acteurs du numérique, dont les utilisateurs sont souvent inconscients et naïfs. En effet,

---

390 Lanna Maximilien, « La protection des données à caractère personnel à l'épreuve de l'automesure connectée », Thèse, Strasbourg, 2019, p. 132.

391 Association française des Correspondants à la protection des données à caractère personnel (AFCDP), « Quantified Self connecté », Informatique & Libertés, novembre 2015, version 10.3 finale, p. 18.

392 Jeunehomme Marie, « L'industrie innovante dans le secteur de l'e-santé face aux défis des régulations », *in* Frison-Roche Marie-Anne, *Internet, espace d'interrégulation*, éd. Dalloz, 2016, p. 90.

393 Lanna Maximilien, *op. cit.*, p. 174.

394 Douville Thibault, « Les dangers de la collecte des données de santé par les tiers intéressés (gafam, assureurs…) », Journal du Droit de la Santé et de l'Assurance, n° 20, 2018, p. 12 : « À l'inverse la puissance économique de ces acteurs, le risque de privatisation de la santé ou d'"uberisation" des acteurs traditionnels, la remise en cause des politiques publiques ou les risques importants d'atteinte à la vie privée des individus font naître des inquiétudes. Pensons à Grindr, ce site de rencontre qui a collecté et partagé le statut sérologique de ses membres et a rendu ces données publiques. ».

les données ne sont pas stockées sur les smartphones des utilisateurs mais bien sur les serveurs des entreprises.

127. Les « données scolaires » ou « données d'éducation ». Il existe d'autres catégories de données qui pourraient être intégrées dans la catégorie des données sensibles. En effet, les données dites « données scolaires » ne font pas l'objet d'une définition propre dans la législation actuelle : il s'agit de données « recueillies dans le cadre scolaire[395] ». La définition mériterait d'être réécrite dans des termes moins généraux afin de prendre en compte les risques de discrimination[396]. Dans ce cadre, afin de prendre en compte les données numériques liées à l'éducation, un comité d'éthique pour les données d'éducation a été instauré en octobre 2019. Le comité a pour mission de conduire une réflexion sur les enjeux éthiques liés aux données d'éducation. Le comité a instauré une définition des données d'éducation comme suit « une donnée numérique personnelle liée à la vie scolaire et concernant différents acteurs de la communauté éducative[397] ». Au sein de cette définition, il ressort deux catégories de données : les données principales et les données accessoires. Les données principales d'éducation concernent les données relatives aux résultats scolaires, aux activités scolaires, au nombre d'élèves et leurs noms et les données relatives au cursus scolaire (historique des formations suivies par un élève et son NIR). Pour les données accessoires d'éducation, il s'agit des données comportementales d'un élève, les données extra-scolaires, les données dérivées des données principales et les données d'accès au service scolaire. Les données d'éducation couvrent donc un large champ puisqu'il s'agit du champ pédagogique et du champ extra-pédagogique[398].

128. Regroupement des données scolaires. Malgré la pluralité des sources des données d'éducation, ces données ne sont pas considérées en principe comme des données sensibles. Les données d'éducation sont protégées en tant que données à caractère personnel de mineurs nécessitant une protection particulière[399], ou en tant que données sensibles lorsqu'il s'agit de

---

395 Braun Gilles, Aristide Cavaillès Jean, Moulet Jean Marc *et al.,* « Données numériques à caractère personnel au sein de l'éducation nationale », Rapport n° 2018-016, février 2018.

396 Martial-Braz Nathalie, Rochfeld Judith et Brogli Marine (dir.), *op. cit*., p. 113.

397 Braun Gilles, Aristide Cavaillès Jean, Moulet Jean Marc *et al*., *op. cit*.

398 Sonnac Nathalie *et al*., « Rapport d'activité du comité d'éthique sur les données d'éducation », 2020-2021.

399 Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), considérant 38 : « Les enfants méritent une protection spécifique en ce qui concerne leurs données à caractère personnel parce qu'ils peuvent être moins conscients des risques, des conséquences et des garanties concernées et de leurs droits liés au traitement des données à caractère personnel. Cette protection spécifique devrait, notamment, s'appliquer à l'utilisation de données à caractère personnel relatives aux enfants à des

données de santé. Pourtant, à l'instar des données de bien-être, avec l'interconnexion des données il sera possible d'effectuer des croisements de données, révélant ainsi des informations sensibles. Par exemple le croisement des données d'absence d'un élève avec le calendrier des fêtes religieuses pourra déterminer la religion de cet élève. Le croisement de données transforme ainsi la donnée d'éducation en une donnée sensible. L'interconnexion de ces données peut s'avérer discriminante pour la future carrière de certains élèves. De surcroît, la masse des données d'éducation a considérablement augmenté avec le confinement et la pratique des enseignements à distance[400].

129. La donnée « preuve[401] ». Toujours dans le domaine des données potentiellement sensibles, une nouvelle notion de donnée est apparue afin de prendre en compte les données à caractère personnel de nature pénale. En effet, la Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes, dite « Directive Police-Justice » a été transposée en France au sein du chapitre XIII de la Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés Informatique et libertés. Le traitement des données à caractère personnel relatives aux condamnations pénales et aux infractions est prévu à l'article 10 du RGPD, indépendamment des autres catégories de données sensibles. L'objectif étant de fixer des règles « spécifiques relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les

fins de marketing ou de création de profils de personnalité ou d'utilisateur et à la collecte de données à caractère personnel relatives aux enfants lors de l'utilisation de services proposés directement à un enfant. Le consentement du titulaire de la responsabilité parentale ne devrait pas être nécessaire dans le cadre de services de prévention ou de conseil proposés directement à un enfant. ».

[400] Rapport précité : « Dans le contexte du confinement ont été produites et traitées de façon massive un grand nombre de données sur les élèves, par exemple toutes les informations sur leur identité insérées dans des plateformes numériques (institutionnelles ou non), ainsi que les travaux échangés entre eux par le biais de ces plateformes (que ce soit des exercices ou des activités en ligne, ou des photos/scans de travaux nécessaires au suivi pédagogique à distance). », p. 28.

[401] Terme utilisé par Frédérique Michéa dans son article « L'appréhension de la donnée en droit de l'Union européenne », *in* Nevejans Nathalie, *Données et technologies numériques*, éd Mare et Martin, 2021, pp. 37-40.

menaces pour la sécurité publique et la prévention de telles menaces, en respectant la nature spécifique de ces activités[402] ».

À ces fins, le traitement de ces données à caractère personnel bénéficie d'un régime dérogatoire au regard des finalités poursuivies. En effet, les données concernées sont des données particulières, liées à des actes sanctionnés pénalement[403]. Les données sont donc soumises à un régime particulier et plus protecteur en raison de l'ingérence particulièrement grave pour le respect de la vie privée et des données à caractère personnel[404]. En substance, les données relatives aux infractions et aux condamnations pénales ne sont pas définies par le RGPD ou le droit interne. Néanmoins la Commission européenne instaure dans le Règlement (UE) 2023/1543 du Parlement européen et du Conseil du 12 juillet 2023 une typologie de données à caractère personnel absente RGPD[405] : il s'agit des données relatives aux abonnés, des données relatives à l'accès, des données relatives aux transactions et des données relatives au contenu[406]. La proposition justifiait ces différentes catégories de données par le fait que cette distinction existe (excepté pour les données relatives à l'accès) dans le droit de nombreux États membres, ainsi qu'aux Etats-Unis. De fait, pour chaque catégorie de données en raison du degré d'interférence différent avec les droits fondamentaux, des conditions différentes sont imposées pour obtenir des données relatives aux abonnés et à l'accès d'une part, et des données relatives aux transactions et au contenu d'autre part.

---

[402] Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, considérant 11.

[403] Douville Thibault, *Droit des données à caractère personnel*, éd. LGDJ, 2023, p. 114.

[404] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), article 10 : « Le traitement des données à caractère personnel relatives aux condamnations pénales et aux infractions ou aux mesures de sûreté connexes fondé sur l'article 6, paragraphe 1, ne peut être effectué que sous le contrôle de l'autorité publique, ou si le traitement est autorisé par le droit de l'Union ou par le droit d'un État membre qui prévoit des garanties appropriées pour les droits et libertés des personnes concernées. Tout registre complet des condamnations pénales ne peut être tenu que sous le contrôle de l'autorité publique. ».

[405] Règlement (UE) 2023/1543 du Parlement européen et du Conseil du 12 juillet 2023 relatif aux injonctions européennes de production et aux injonctions européennes de conservation concernant les preuves électroniques dans le cadre des procédures pénales et aux fins de l'exécution de peines privatives de liberté prononcées à l'issue d'une procédure pénale.

[406] Michéa Frédérique, « L'appréhension de la donnée en droit de l'Union européenne », *in* Nevejans Nathalie, *Données et technologies numériques,* éd. Mare et Martin, 2021, p. 38.

130. Les « données altruistes ». Récemment, le Règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données (règlement sur la gouvernance des données), dit « DGA », instaure un nouveau type de donnée : la donnée altruiste. Il s'agit de données volontairement mises à disposition par des particuliers ou des entreprises pour le bien commun. Les données sont mises à disposition sans aucune contrepartie à des fins d'intérêt général, telles que la recherche scientifique ou l'amélioration des services publics[407]. L'altruisme des donnés permet de redynamiser la politique d'ouverture des données en renouvelant l'approche de l'intérêt général. En effet, l'*open data* et l'altruisme des données se rejoignent dans la notion partage des données tout en ayant une conception différente de l'intérêt général[408]. Dans l'altruisme des données, l'intérêt général repose sur le volontariat des différents acteurs : le générateur, le détenteur, l'utilisateur, l'intermédiaire et pour finir, le tiers de confiance qui vérifie l'altruisme de la donnée. Le mouvement d'altruisme des données va permettre d'augmenter le volume des données disponibles à des fins d'intérêt général afin de faciliter le développement de solutions d'analyse de données[409].

131. Les données d'intelligence artificielle. Pour finir, le Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle a instauré une nouvelle typologie de données propre à l'intelligence artificielle : les « données de validation », les « données de test », les « données d'entrée » et les « données d'entraînement ». Le règlement prend le soin de définir ces différents types de données. Les données d'entrée sont simplement les données fournies à un système d'intelligence artificielle ou directement acquises par le système à partir desquelles il produit un résultat[410]. Les données d'entraînement sont les données utilisées pour entraîner le système en ajustant ses paramètres[411]. En pratique, lorsque ces systèmes reposent sur

[407] Règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données (règlement sur la gouvernance des données), article 2 point 10.
[408] Favro Karine, « Transformation numérique de l'administration », Répertoire de service publique, Dalloz, avril 2023.
[409] Fontaine Quentin et Strowel Alain, « La stratégie européenne pour les données », *in* Bertrand Brunessen (dir.), *La politique européenne du numérique*, éd. Bruylant, 2023, p. 723 : « Elle [La Commission] identifie certains domaines propices au partage altruiste, en particulier les soins de santé, la lutte contre le changement climatique et la mobilité. L'attente est donc que l'altruisme contribue à alimenter les réserves communes nécessaires au développement des espaces européens de données dans chacun des secteurs ».
[410] Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle, article 3, point 32.
[411] *Ibid*., article 3, point 29.

l'apprentissage automatique, le choix des données d'entraînement est primordial[412]. Les données de validation sont quant à elles définies comme des données utilisées pour évaluer le système d'intelligence artificielle et pour ajuster les paramètres non entraînables et son processus d'apprentissage[413]. Et enfin, les données de test sont des données qui permettent d'évaluer le système – déjà validé et entraîné – pour confirmer ses performances attendues avant sa mise en marché ou en service[414]. *In fine*, la qualité de ces données est fondamentale afin de garantir des systèmes d'intelligence artificielle fiables et transparents.

Ainsi, plusieurs notions sont instaurées par le législateur ou s'imposent par la pratique. La catégorie des données à caractère personnel et non personnel n'est pas exclusive, les données publiques ont également pris une place considérable au sein de la typologie. Avec le développement de l'ouverture des données, la notion de donnée publique devient inéluctable.

II. La construction de la notion des « données publiques »

132. Une notion complexe. La notion de donnée publique est une notion complexe à définir (A). Pour autant, la valeur des données étant une valeur d'usage, le législateur n'hésite pas à instaurer de nouvelles catégories concurrentes afin de promouvoir l'ouverture des données (B).

A) La définition stricte de la donnée publique

133. Contexte et contours de la notion. Dans le dessein de définir la donnée publique, il convient d'en préciser le contexte (1) afin de pouvoir dessiner les contours de la donnée publique (2).

---

[412] Bertrand Brunessen, « La gouvernance des données dans la régulation européenne de l'intelligence artificielle », RTD eur., 2022, n° 315 : « La qualité des données détermine le bon fonctionnement de nombreux systèmes d'IA, en particulier pour les technologies fondées sur l'entraînement de modèles. Dès lors que ces systèmes reposent sur l'apprentissage automatique, le choix des données d'entrainement est fondamental du point de vue de leur représentativité et de leur pertinence par rapport à la finalité de l'application. ».

[413] Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle, article 3, point 30.

[414] *Ibid*., article 3, point 31.

1. Contexte de la donnée publique

134. Production des données publiques. Les données publiques ne sont pas une « réalité nouvelle[415] ». Le fait que l'État utilise et produit d'importants volumes de données afin de mener l'action publique n'est pas nouveau. Les données publiques servent à l'administration comme une aide à la prise de décision[416], par exemple pour les projets d'aménagements ou pour évaluer les politiques mises en œuvre. Les données publiques sont également essentielles au fonctionnement des services du quotidien, des transports à la vie culturelle en passant par les crèches ou les écoles. Avec l'essor de la numérisation, le volume des données produites par l'État a changé d'échelle et la nature des données a évolué[417]. Les données publiques sont produites par des acteurs variés et sont utilisées pour un grand nombre de finalités[418]. Une donnée produite par l'administration pour servir ses propres besoins peut s'avérer utile à d'autres acteurs. Ainsi, la numérisation a permis d'étendre le champ de la donnée publique afin de la rendre plus facilement accessible.

135. Définition d'une donnée ouverte. Contrairement à la notion de donnée publique, la notion « donnée publique ouverte » ignore le contexte de production et ses spécificités pour se préoccuper de l'usage et l'interopérabilité des données[419]. En pratique, les données publiques publiées en ligne ne sont pas forcément « ouvertes » : toutes les données publiques ne sont pas ouvertes, et toutes les données ouvertes ne sont pas publiques[420]. Pour qu'une donnée puisse être qualifiée d'ouverte, elle doit répondre à un ensemble de critères techniques, juridiques et économiques[421]. La donnée est ouverte lorsqu'elle est diffusée de manière structurée, en libre accès, sans restriction technique ou financière. D'une façon générale, la donnée ouverte est une « donnée numérique d'origine publique ou privée, produite par une collectivité dans le cadre de l'exploitation d'un service public, par une entreprise ou un individu[422]». La diffusion des données

[415] Chevallier Jacques et Cluzel-Métayer Lucie, « Introduction », Revue française d'administration publique, n° 167, École nationale d'administration, 2018.
[416] Chignard Simon, *Open data*, éd. FYP, 2012, p. 10.
[417] Hoang Mathilde, « Les données publiques : qu'en est-il de leur ouverture et de leur réutilisation ? », Cahiers Français, 2021.
[418] Favro Karine, « "Les données non personnelles" : un nouvel objet juridique », Dalloz IP/IT, 2020.
[419] Teresi Laurent, « L'open data et le droit de l'Union européenne », AJDA, 2016, 87.
[420] Boul Maxime, « Réflexions sur la notion de donnée publique », Revue française d'administration publique, n° 167, École nationale d'administration, 2018, pp. 471-478.
[421] Chignard Simon, *op. cit.*, p.14.
[422] Favro Karine, « Introduction », Légicom, 56, 2016.

ouverte est assurée par une licence ouverte garantissant son libre accès et sa réutilisation par tous. Ainsi, dès lors que la donnée est ouverte, elle devient une potentielle source de valeur pour tout acteur, public comme privé.

136. Valeur des données publiques. La politique publique d'ouverture des données s'est progressivement mise en place par le mouvement d'*open data*. Il s'agit tout à la fois d'une politique d'ouverture des données et du développement des données ouvertes. Le mouvement d'ouverture des données est une étape supplémentaire et nécessaire à la création de valeur dans une économie numérique[423]. En effet, la transformation de l'administration permet de valoriser la donnée publique et d'exploiter la valeur de ces données. La politique va permettre à de nombreux acteurs d'utiliser les données publiques à d'autres fins que celles initialement prévues par l'administration. La valeur de la donnée étant principalement une valeur d'usage, les données publiques sont davantage valorisées lorsqu'elles peuvent être réutilisées par plusieurs acteurs. Ainsi, l'*open data* permet d'exploiter la valeur d'usage des données publiques et de créer de la valeur en réutilisant les données mises à disposition par l'administration. De ce fait, l'ouverture des données permet d'explorer la valeur de réutilisation des données et de promouvoir l'innovation[424].

137. Promotion et bénéfices de l'*open data*. De façon pédagogique, OpenDataFrance[425] présente sur son site les possibles cas de réutilisation des données publiques. Sur le site, plusieurs dossiers thématiques permettent de démontrer l'utilité de l'usage des données publiques. À titre d'illustration, la société Street-co est à l'origine d'un GPS piéton collaboratif : l'application permet de calculer des itinéraires sans obstacles pour les personnes handicapées. À l'instar de l'application Waze qui s'appuie sur une communauté d'utilisateurs, l'application Street-co permet d'avoir des données à jour et en temps réel. L'usage des données ouvertes s'avère bénéfique dans de nombreux domaines comme la physique, la santé, l'environnement ou encore les sciences humaines[426]. Particulièrement, l'ouverture des données est indispensable pour étudier et combattre le réchauffement climatique. En outre, l'intérêt d'ouvrir les données publiques a été confirmé lors de l'épidémie mondiale de la Covid19. Dans le cadre de la politique d'*open data*, le gouvernement français a publié des données en temps réel sur la

423 *Ibid*.
424 Chignard Simon et Benyayer Louis-David, *Datanomics,* éd. FYP, 2015, p. 126.
425 v. https://www.opendatafrance.net/reutilisations/
426 Verdier Henri et Vergnolle Suzanne, « L'État et la politique d'ouverture en France », AJDA, 2016, 92.

pandémie[427]. L'ouverture de ces données a permis une meilleure gestion de la crise sanitaire et la diffusion de l'information. L'intérêt de l'*open data* des données publiques n'est plus à démontrer. Pour autant, la notion de donnée publique est encore à parfaire.

2. Notion de donnée publique

138. Définition de la donnée publique. La notion de donnée publique est prégnante dans le contexte de l'*open data.* Néanmoins, les références aux données publiques se sont multipliées ces dernières années sans pour autant devenir une véritable notion juridique. La catégorie juridique des données publiques ne se présente pas comme une catégorie homogène. Tout d'abord, la circulaire du 14 février 1994 relative à la diffusion des données publiques faisait référence d'une part, à une définition étroite de la donnée publique comme « une information formatée pour être traitée par un système informatique », et d'autre part, à une définition large de la donnée publique comme une « information collectée ou produite sur n'importe quel support, pas seulement informatique »[428]. Avec l'essor de la numérisation, la distinction tend à s'effacer afin de devenir des « informations mises en forme pour être traitées informatiquement[429] ». En effet, l'article L.321-1 du CRPA, évoque des « informations publiques figurant dans les documents communiqués ou publiés par les administrations[430] ». Ainsi, à l'instar de la donnée à caractère personnel, les données publiques sont des informations.

139. Le caractère « public ». Le caractère « public » des données n'est pas lié au rattachement d'une personne publique mais réside dans la « mission de service public dans le cadre de laquelle les données ont été produites, recueillies ou détenues[431] ». Ainsi, le caractère « public » des données est rattaché au critère matériel du service public, critère prépondérant au critère organique impliquant la présence d'une personne publique. Sur ce point, la circulaire de 1994 était équivoque puisque la diffusion des données publiques visait « l'activité d'une

[427] Le site data.gouv.fr référence les principaux jeux de données relatifs à la Covid 19. Disponible à l'adresse : https://www.data.gouv.fr/fr/pages/donnees-coronavirus/

[428] Circulaire du 14 février 1994 relative à la diffusion des données publiques.

[429] Boul Maxime, « Réflexions sur la notion de donnée publique », Revue francaise d'administration publique, n° 167, École nationale d'administration, 2018.

[430] Code des relations entre le public et l'administration, article L321-1 : « Les informations publiques figurant dans des documents communiqués ou publiés par les administrations mentionnées au premier alinéa de l'article L. 300-2 peuvent être utilisées par toute personne qui le souhaite à d'autres fins que celles de la mission de service public pour les besoins de laquelle les documents ont été produits ou reçus. ».

[431] Code des relations entre le public et l'administration, article L300-2.

personne publique ». L'article 300-2 du CRPA met fin à cette ambiguïté en visant les personnes privées chargées d'une mission de service public.

Ainsi, par dichotomie, toute donnée qui n'est pas une donnée publique est une donnée privée. Pour autant, cette distinction n'est pas évidente en pratique puisque la législation ne cesse d'introduire des définitions concurrentes à la notion de donnée publique.

B) Les définitions concurrentes à la notion de donnée publique

140. Introduction de nouvelles notions. La Loi n° 2016-1321 du 7 octobre 2016 pour une République a introduit de nouvelles notions afin de renforcer l'ouverture des données publiques : la notion de « données de référence » (1) et la notion de « données d'intérêt général » (2).

1. La notion de « données de référence »

141. Définition des « données de référence ». La notion recouvre les informations qui « constituent une référence commune pour nommer ou identifier des produits, des services, des territoires ou des personnes », qui sont « réutilisées fréquemment par des personnes publiques ou privées autres que l'administration qui les détient » et dont « leur réutilisation nécessite qu'elles soient mises à disposition avec un niveau élevé de qualité[432] ». Les données de référence sont des informations publiques particulières. En effet, selon l'article L.321-4 du CRPA, elles peuvent être utilisées par toute personne qui le souhaite à d'autres fins que celles de la mission de service public pour les besoins de laquelle les documents ont été produits ou reçus[433]. Les données de référence peuvent avoir d'autres usages, d'où la nécessité de faciliter leur accessibilité.

142. Création d'un service public de la donnée. La notion de données de référence a été intégrée pour contribuer à la création d'un service public de la donnée[434], service ayant pour objectif de faciliter la réutilisation des données publiques. L'article précité précise que « la mise

[432] Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique, article L321-4.

[433]Code des relations entre le public et l'administration, article L321-4, I ; Cluzel-Métayer Lucie, « La construction d'un service public de la donnée », Revue française d'administration publique, n° 167, École nationale d'administration, 2018.

[434] Chevallier Jacques, « Vers l'État-plateforme ? », Revue française d'administration publique, n° 167, École nationale d'administration, 2018, p. 630.

à disposition des données de référence en vue de faciliter leur réutilisation constitue une mission de service public relevant de l'État ». Le service public relève donc de l'État auquel toutes les administrations doivent participer. Le rôle du service public de la donnée « n'est pas de créer de nouvelles données, mais de constituer, dans un univers de données très dense et dont les sources ne sont pas toujours identifiables ou maitrisées, une ressource fiable et authentifiée par la puissance publique[435] ». Le service public de la donnée a pour mission de développer la circulation des données ayant un impact économique et social, afin de pouvoir concevoir de nouveaux services.

143. Mise en œuvre du service public de la donnée. Le service public de la donnée est organisé de la façon suivante : des producteurs émettent les données de référence ou documentent les métadonnées. Ensuite, les diffuseurs mettent à disposition les données de référence avec un haut niveau de qualité et les utilisateurs peuvent utiliser ces données de référence pour de nouveaux usages. Les utilisateurs participent à la qualité de ces données en signalant les erreurs et en faisant des propositions d'amélioration. La mise en œuvre de ce service public de la donnée a été confiée à la mission Etalab, en charge du portail data.gouv.fr qui recense l'ensemble des jeux de données de référence. Les jeux de données sont des données pivots dont l'objectif est de les relier entre elles pour les enrichir[436].

À ce jour, le service public de la donnée met à disposition neuf bases de données de référence : la Base Adresse Nationale (BAN), la base Siren des Entreprises et de leurs établissements (SIREN), le Plan Cadastre Informisé (PCI), le Code Offiel géographique (COG), le Registre Parcellaire Graphique (RPG), le référentiel de l'organisation administrative de l'Etat, le Référentiel à Grande Echelle (RGE), le Répertoire National des Associations (RNA) et le Répertoire opérationnel des métiers et des emplois (Rome)[437]. Les données de référence sont surtout des données de qualité, qui sont à la fois un levier économique, un outil d'amélioration de l'action publique et du service rendu aux citoyens[438]. De manière concrète, l'utilisation d'un même référentiel d'adresses permet une meilleure coordination et donc efficacité de l'intervention des services d'urgence ou de secours.

---

435 Étude d'impact du projet de loi « Pour une République numérique », 9 décembre 2015.

436 Boul Maxime, « Réflexions sur la notion de donnée publique », Revue française d'administration publique, n° 167, École nationale d'administration, 2018.

437 Code des relations entre le public et l'administration, article R321-5 : « Le service public des données de référence met à la disposition du public les données suivantes : […] ».

438 Cluzel-Métayer Lucie, *op. cit*.

Afin d'ouvrir davantage de données dans un contexte d'*open data*, le législateur français a également instauré la notion de « donnée d'intérêt général ».

2. La notion de « données d'intérêt général »

144. Définition opaque de la « donnée d'intérêt général »[439]. À l'instar de la notion de « données de référence », la notion de « donnée d'intérêt général » a été introduite par la Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique aux articles 17 à 24. Pour autant, la notion de « données d'intérêt général » ne fait pas l'objet d'une réelle définition. Les données d'intérêt général peuvent être des données publiques ou privées, dont le partage et l'ouverture sont « d'intérêt général », c'est-à-dire un intérêt plus large que le seul intérêt du détenteur des données[440]. Le rapport « Pour une politique publique de la donnée » définit ces données comme des données qui permettent « de décrire, d'éclairer voire d'agir pour l'intérêt général, même si elles ont été produites ou collectées par la sphère privée[441] ». Ainsi, le caractère privé du détendeur des données ne suffit pas à faire obstacle au partage et à l'ouverture de ces données. La notion « d'intérêt général » permet d'englober toutes les données qui portent une atteinte toute relative à la liberté d'entreprendre en raison de leur caractère non-rival[442]. Aujourd'hui, le champ de la notion est particulièrement large et peut comporter les données de l'État, des collectivités locales et des autres organismes de droit public, des entreprises publiques et des données de recherche financée par des fonds publics[443]. Dans le cadre de sa stratégie sur les données, la Commission cherche également à promouvoir le partage entre entreprises[444].

Les données d'intérêt général sont des données qui ne sont pas des « données de référence », mais considérées comme des données particulièrement stratégiques. Par-delà les données publiques diffusées en *open data*, certaines données privées peuvent être source de valeur économique et/ou sociétale importante. Les données ayant une valeur d'usage, certaines données privées doivent pouvoir être réutilisés. Le rapport précité précise qu'il en est ainsi

---

439 Boul Maxime, *op. cit*.

440 Pailhès Bertrand, « Comment définir et réguler les « données d'intérêt général » ? », Annales des Mines, 2018.

441 Misson Bothorel, « Pour une politique publique de la donnée », 2020.

442 Favro Karine, « "Les données non personnelles" : un nouvel objet juridique », Dalloz IP/IT, 2020.

443 Cytermann Laurent, « L'ouverture des donnes publiques en Europe : principes et nouvelles frontières », *in* Bertrand Brunessen (dir.), *La politique européenne du numérique*, éd. Bruylant, 2023, p. 394.

444 Commission européenne, « Une stratégie européenne pour les données », COM(2020) 66 final, 19 février 2020.

lorsque « l'ouverture de ces données détenues par des personnes privées peuvent concourir à l'intérêt général, permettant une conduite plus efficace de politiques publiques sectorielles, en assurant une meilleure information des citoyens, en concourant à la recherche scientifique, ou en bénéficiant au développement économique[445] ».

145. Distinction. L'ouverture et le partage des données d'intérêt général permettent l'amélioration des politiques publiques[446]. Pour autant, les données d'intérêt général doivent être distinguées de la notion d'*open data* qui trouve sa source à travers un droit constitutionnel pour le citoyen envers l'administration. Les données d'intérêt général sont soumises à des conditions particulières d'accessibilité et ne font pas l'objet d'un droit fondamental. De surcroît, les données d'intérêt général deviennent des données publiques soumises à la politique d'ouverture une fois seulement leur mise à disposition. Ainsi, les données d'intérêt général peuvent être qualifiées de « données publiques par destination[447]». Dès lors que ces données peuvent avoir comme finalité l'intérêt général, elles font l'objet de régime d'exclusivité aménagé. La loi prévoit les modalités et conditions de réutilisation et publication propres à chaque catégorie de donnée d'intérêt général. Afin de permettre l'efficacité du partage et de l'ouverture de ces données par des acteurs privés, l'accès aux données d'intérêt général ne doit pas nécessairement être gratuit mais fixé à un prix raisonnable, incitant le détenteur à investir[448].

146. Diversité des données. En réalité, les données d'intérêt général sont un ensemble de données hétérogène. Les domaines particulièrement concernés sont les transports, la mobilité, l'énergie, l'environnement et la santé[449]. Plus précisément, il peut s'agir de données relatives aux conventions de subventions publiques attribuées dans le cadre d'un service public et commercial, de données relatives à la consommation énergétique, aux valeurs foncières, aux vitesses maximales autorisés sur le domaine public routier, des données de base de données reçues ou produites à l'occasion de l'exploitation du service public faisant l'objet d'un contrat de concession et qui sont indispensables à son exécution[450]. Il s'agit aussi des données publiques

---

445 Aureau Tristan, Cytermann Laurent, Duchesne Claudine, Morel Mathieu, Vachey Laurent, « Rapport relatif aux données d'intérêt général », Rapport d'étape, septembre 2015.
446 *Ibid*.
447 Cassar Bertrand, « Gouvernance des données », Encyclopédie Dalloz : NTIC et IP/IT, 2022.
448 Pailhès Bertrand, *op. cit*.
449 Boillet Nicolas, Baranes Edmond, Sauron Jean-Luc et *al*., « Le règne des données », Cahiers français, 419, 2021, p. 22.
450 Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique, articles 17 et 18.

qui concernent des personnes privées « lorsqu'elles participent de près ou de loin, à un service public[451] », comme les données jurisprudentielles et l'ouverture des données scientifiques[452].

Le directeur des Technologies et de l'Innovation à la Commission nationale de l'informatique et des libertés, Bertrand Pailhes, estime que le meilleur exemple pour illustrer l'intérêt des données d'intérêt général est l'exemple des transports. Pour lui, dans ce secteur, les données sont abondantes, l'utilité de leur collecte massive peut servir à traiter des problèmes quotidiens tels que les embouteillages, la pollution de l'air ou le fonctionnement des transports publics. Elles sont collectées par une grande variété d'acteurs, et le secteur est l'objet de l'attention de nouveaux acteurs au regard de l'intérêt pour les utilisateurs pour des applications comme Google Maps ou Waze. Ainsi, « l'enjeu de l'accès aux données est donc double : d'une part développer une activité économique en soutenant l'innovation et en évitant la constitution de rentes et, d'autre part, améliorer la conduite des politiques publiques[453] ».

147. Création de la notion de « données à forte valeur ». La Directive (UE) 2019/1024 du Parlement européen et du Conseil du 20 juin 2019 concernant les données ouvertes et la réutilisation des informations du secteur public dispose que les données du secteur public ou provenant de financements publics doivent être réutilisables par défaut. Pour ce faire, la directive introduit la notion d'« ensembles de données de forte valeur »[454]. L'article 2, point 10 précise que ces données sont « des documents dont la réutilisation est associée à d'importantes retombées positives au niveau de la société, de l'environnement et de l'économie, en particulier parce qu'ils se prêtent à la création de services possédant une valeur ajoutée, d'applications et de nouveaux emplois décents et de grande qualité, ainsi qu'en raison du nombre de bénéficiaires potentiels des services et applications à valeur ajoutée fondés sur ces ensembles de données ». Les données de forte valeur sont librement et gratuitement réutilisables. L'annexe 1 de la directive propose six catégories de données à forte valeur tels que les informations relatives aux secteurs géospatiaux, météorologiques, statistiques, aux entreprises et leur propriété, à la mobilité ainsi qu'à l'observation de la terre et de l'environnement. Cette liste pouvant être

[451] Cluzel-Métayer Lucie, « La loi pour une République numérique : l'écosystème de la donnée saisi par le droit », AJDA, 2017.
[452] *Ibid.*
[453] Pailhès Bertrand, *op. cit.*
[454] Directive (UE) 2019/1024 du Parlement européen et du Conseil du 20 juin 2019 concernant les données ouvertes et la réutilisation des informations du secteur public.

modifiée par un acte délégué de la Commission européenne « afin de refléter les progrès technologiques et l'évolution du marché[455] ».

In fine, les ensembles de données à forte valeur sont très proches des données d'intérêt général, illustrant l'influence normative française sur la législation européenne[456]. Pour autant, contrairement aux données de référence, les données à forte valeur peuvent faire l'objet de dérogations concernant le principe de gratuité[457].

148. Introduction de la notion de « données dynamiques ». De surcroît, ladite directive a également introduit la notion de « données dynamiques ». Les données dynamiques sont « des documents présentant sous forme numérique et faisant l'objet d'actualisations fréquentes ou en temps réel, notamment à cause de leur volatilité ou de leur obsolescence rapide » ou encore des données « émanant de capteurs[458] ». Cette notion de « données dynamiques » apparaissait dans un règlement du 15 mai 2013 sur la mise à disposition de services d'informations concernant les aires de stationnement[459]. Le règlement évoquait des « données dynamiques sur la disponibilité des aires de stationnement, en particulier si une aire de stationnement est complète ou fermée, ou encore le nombre de places disponibles[460] ». Ainsi, à la différence des données ouvertes dans le cadre de l'*open data*, les données dynamiques sont transmises en temps réel. Au final, les données à forte valeur sont des données dynamiques[461].

[455] *Ibid*., article 13.
[456] Petel Antoine, « Politique sur les données : comparaison des approches française et européenne », sur IDFRights .
[457] *Ibid*., article 14.
[458] *Ibid.*, article 2, point 8.
[459] Règlement délégué (UE) n° 885/2013 de la Commission du 15 mai 2013 complétant la directive 2010/40/UE du Parlement européen et du Conseil (directive «STI») en ce qui concerne la mise à disposition de services d'informations concernant les aires de stationnement sûres et sécurisées pour les camions et les véhicules commerciaux.
[460] *Ibid*., article 4 point 3.
[461] Cassar Bertrand, *op. cit*.

149. Conclusion de la section. Au regard de l'usage des données, le législateur a saisi les données comme nouvel objet de droit en établissant une typologie des données. La typologie des données permet de déterminer un régime propre à chaque type de donnés. Selon la nature ou selon les risques, la donnée fera l'objet d'un régime de protection ou d'ouverture. L'instauration d'une typologie stable et précise est donc fondamentale.

Pour les données à caractère personnel, la définition est volontairement extensive afin de protéger efficacement les utilisateurs contre les dérives des acteurs du numérique. Les données à caractère personnel visent toute information relative à une personne physique, identifiée ou identifiable. La catégorie de données à caractère personnel comporte des sous-catégories, comme les données sensibles. En pratique, la qualification de personnel entraîne *de facto* le régime de protection. Par opposition, les données à caractère non personnel représentent simplement toutes les données autres que les données à caractère personnel. Il s'agit d'une définition par dichotomie avec les données à caractère personnel.

Enfin, les données publiques font l'objet d'une typologie propre, selon le potentiel d'usage des données. En effet, toutes les données publiques n'ont pas la même valeur d'usage. Dans ce domaine, le législateur a été précurseur en intégrant les données d'intérêt général et les données de référence, données de qualité. Dans l'ensemble des domaines, le partage et l'ouverture des données sont nécessaires dans une société axée sur les données. Le potentiel de l'ouverture des données doit être utilisé pour la crise environnementale.

Pour autant, la dualité promise entre données à caractère personnel et données à caractère non personnel n'est pas si simple. Les technologies émergentes font apparaître de nouvelles notions de données, comme les données de bien-être : ces dernières sont nombreuses avec le développement de la quantification de soi. En pratique, il s'agit principalement de données relatives à la santé des utilisateurs. Avec le *Big Data* et les techniques de corrélations, ces données s'avèrent particulièrement dangereuses pour la vie privée des individus.

En réalité, lorsque les données ne sont pas rigoureusement définies, l'incertitude profite aux géants du numérique. *A contrario*, l'excessive diversité de notions impacte l'intelligibilité du cadre. Les acteurs du numérique profitent de cette multiplicité. Par ailleurs, les technologies émergentes démontrent malencontreusement les faiblesses de la typologie instaurée.

Section 2 : L'instabilité de la typologie

150. Protection et ouverture des données. Le droit dérivé a instauré une typologie des données selon leur nature. La nature des données instaure un régime spécifique pour chaque type de données selon l'opportunité ou les risques. Les données à caractère personnel font donc l'objet d'une protection particulière au regard des dangers pour les personnes physiques. Au contraire, la libre circulation des données à caractère non personnel et l'ouverture des données publiques par défaut deviennent la norme.

151. Essor de l'intelligence artificielle. À l'ère du *Big Data*, la frontière entre les données à caractère personnel, les données à caractère non personnel et les données publiques n'est pas toujours assurée. Avec l'essor des objets connectés et de l'intelligence artificielle les ensembles de données sont majoritaires et entraînent un chevauchement des notions (I). Afin de contrer les risques pour les individus, l'anonymisation des données devient la règle pour pouvoir partager certaines données. En réalité, le contexte technologique affaiblit les techniques d'anonymisation (II).

I. Le chevauchement des notions

152. Frontières poreuses entre les notions. Afin de développer le potentiel des données, la libre circulation des données à caractère non personnel est devenue la cinquième liberté économique dans l'Union européenne. Le potentiel des données à caractère non personnel est indéniable dans une stratégie de marché unique numérique. En pratique, un certain nombre de données outrepassent la frontière entre données à caractère personnel et données à caractère non personnel (A). En parallèle, l'ouverture des données publiques représente un potentiel pour la société et le partage de la connaissance. Néanmoins, certains documents publics peuvent contenir des données à caractère personnel (B).

A) Les données à caractère personnel et données à caractère non personnel

153. Rencontre des données. La rencontre des données à caractère personnel et des données à caractère non personnel fait apparaître des ensembles de données mixtes (1). Afin de résoudre le conflit entre les différents types de données, le législateur a mis en place une application distributive des règles (2).

1. La notion d'« ensemble de données mixtes »

154. Dichotomie entre données à caractère personnel et données à caractère non personnel. Les données à caractère non personnel sont définies par opposition aux données à caractère personnel. Cette dichotomie pourrait paraître simple : une donnée à caractère non personnel n'est pas une donnée à caractère personnel[462]. Pourtant, en pratique, la détermination du périmètre respectif des données à caractère personnel et des données à caractère non personnel est complexe[463]. D'une part, cette distinction est artificielle pour le technicien : une donnée est une donnée.[464] D'autre part, l'évolution des technologies rend de plus en plus délicate la délimitation entre une donnée à caractère personnel et une donnée à caractère non personnel : les systèmes d'intelligence artificielle rendent complexe l'opération de qualification juridique des données exploitées. Ainsi, il existe des ensembles de données composés à la fois de données à caractère non personnel et de données à caractère personnel.

---

[462] Article 2 du Règlement (UE) 2018/1807 du Parlement et du Conseil du 14 novembre 2018 établissant un cadre applicable au libre flux des données à caractère non personnel dans l'Union Européenne : « 1. Le présent règlement s'applique au traitement de données électroniques autres que les données à caractère personnel dans l'Union, qui est : a) fourni en tant que service aux utilisateurs résidant ou disposant d'un établissement dans l'Union, par un fournisseur de services établi ou non dans l'Union ; ou b) effectué par une personne physique ou morale résidant ou disposant d'un établissement dans l'Union pour ses propres besoins. ».

[463] Castets-Renard Céline, *Droit du marché unique numérique et intelligence artificielle*, éd. Bruylant, 2020, p. 238 : « Eu égard à la large définition de la notion de donnée à caractère personnel et aux technologies disponibles aujourd'hui, il devient de plus en plus difficile de tracer une frontière nette entre les jeux de données comportant des données personnelles et ceux qui n'en comportent pas. ».

[464] Gossa Julien, « Les données non personnelles : un tech checking », Dalloz IP/IT, 2020 : « Non seulement ce problème est en réalité difficile, mais en plus le technicien ne se pose généralement pas cette question, en tous cas pas en ces termes. Ses besoins et intentions sont ailleurs : que le système fonctionne, qu'il soit robuste et efficace, à un coût contenu. La tâche est généralement suffisamment complexe et prenante pour ne pas en ajouter. En réalité, cette distinction, fondamentale pour le juriste, reste, pour le technicien, assez artificielle : une donnée est une donnée. ».

155. Ensemble de données mixtes. Les lignes directrices de la Commission européenne relatives au règlement concernant un cadre applicable au libre flux des données à caractère personnel précisent que dans la pratique - et dans la plupart des cas -, un ensemble de données est composé à la fois de données à caractère personnel et de données à caractère non personnel, qualifié « d'ensemble de données mixtes[465] ». Les données mixtes sont un ensemble de données comportant à la fois des données à caractère personnel et des données à caractère non personnel. Les données mixtes sont majoritaires avec l'essor de l'Internet des objets, l'intelligence artificielle et les technologies permettant l'analyse des mégadonnées.

156. Exemples d'ensembles données mixtes. Dans les lignes directrices précitées, la Commission propose des exemples d'ensembles de données mixtes comme le dossier fiscal d'une entreprise, mentionnant le nom et le numéro de téléphone du directeur général de l'entreprise ; les ensembles de données d'une banque, notamment ceux qui contiennent des informations sur les clients et les détails de transactions, tels que les services de paiement (cartes de crédit et de débit), les applications de gestion des relations avec les partenaires et les conventions de prêt, les documents combinant des données concernant tant des personnes physiques que des personnes morales ; les données statistiques anonymisées d'un établissement de recherche et les données brutes initialement collectées, telles que les réponses des personnes interrogées à des questionnaires d'enquête ; une base de données sur les problèmes informatiques d'une entreprise et leurs solutions fondées sur des rapports individuels d'incidents informatiques ; des données relatives à l'Internet des objets, lorsque certaines des données permettent d'émettre des hypothèses sur des individus identifiables (par exemple, présence à une adresse et modalités d'utilisation particulières) ainsi que l'analyse des données des journaux d'exploitation d'équipements de production dans l'industrie manufacturière[466].

157. Données composites. Pour d'aucuns, le terme de « données mixtes » est erroné car une donnée ne peut revêtir un double caractère, personnel ou non personnel. Il serait préférable de parler d'ensemble de « données composites »[467]. La notion d'ensemble de données mixtes serait promise à une révision afin de prendre en compte l'évolution des technologies ou des marchés.

---

[465] Commission européenne, « Lignes directrices relatives au règlement concernant un cadre applicable au libre flux des données à caractère non personnel dans l'Union européenne », COM(2019) 250 final.

[466] Commission européenne, « Lignes directrices relatives au règlement concernant un cadre applicable au libre flux des données à caractère non personnel dans l'Union européenne », COM(2019) 250 final, p. 9.

[467] Zorn Caroline, « Le jeu de données composites : données personnelles et (en même temps) non personnelles ? », Dalloz IP/IT, 2020.

Par ailleurs, les données peuvent se « métamorphoser » durant un traitement algorithmique[468] : par le biais d'un traitement ou d'un recoupement, les données peuvent revêtir une nature nouvelle. Sans prendre en compte cette possible permutation, les règlements prévoient des règles distributives élémentaires.

2. L'application de règles distributives

158. Champ d'application. Le Règlement (UE) 2018/1807 du Parlement européen et du Conseil du 14 novembre 2018 établissant un cadre applicable au libre flux des données à caractère personnel précise que pour un ensemble de données « composé à la fois de données à caractère personnel et de données à caractère non personnel, le présent règlement s'applique aux données de l'ensemble à caractère non personnel[469] ». De manière cohérente, le RGPD s'applique aux données à caractère personnel sans exception, tandis que les données à caractère non personnel sont soumises au règlement sur le libre flux des données à caractère non personnel.

159. Données inextricablement liées. L'article 2 du Règlement (UE) 2018/1807 du Parlement européen et du Conseil du 14 novembre 2018 établissant un cadre applicable au libre flux des données à caractère personnel poursuit comme tel « lorsque les données à caractère personnel et les données à caractère non personnel d'un ensemble sont inextricablement liées, le présent règlement est sans préjudice de l'application du règlement (UE) 2016/679 ». En pratique, lorsque les données sont inextricablement liées, le RGPD s'applique à l'intégralité des données, même lorsque les données à caractère personnel ne représentent qu'une petite partie de l'ensemble des données. Ainsi, qu'importe la quantité de données à caractère personnel, le Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données prime sur l'ensemble de données. En dépit de la stratégie du marché unique numérique, la protection des individus semble primer sur la libre circulation des données à caractère non personnel.

---

468 Bougeard Aurélien, « L'appréhension juridique du Big Data par sa décomposition technique », *in* Nevejans Nathalie (dir.), *Données et technologies numériques,* éd. Mare et Martin, 2021, p. 125 : « Des données appartenant à l'ensemble de données à caractère non personnel peuvent par le biais d'un recoupement identifier une personne et donc transiter une catégorie ante-traitement à une autre catégorie plus contraignante post-traitement. ».

469 Règlement (UE) 2018/1807 du Parlement européen et du Conseil du 14 novembre 2018 établissant un cadre applicable au libre flux des données à caractère personnel, article 2.

Néanmoins, la notion « d'inextricablement lié » n'est définie par aucun règlement. Les lignes directrices précitées évoquent les situations où une séparation entre les deux serait soit impossible, soit considérée comme économiquement inefficace ou techniquement impossible par le responsable de traitement. En cas d'ensemble de données mixtes, les entreprises ne sont pas soumises à une obligation de séparer les données en fonction de leur nature. Les entreprises peuvent traiter l'ensemble de données mixtes en respectant les régimes applicables. Pour autant, il parait opportun d'anonymiser les données à caractère personnel afin de pouvoir les considérer comme des données à caractère non personnel.

160. Données à caractère personnel anonymisées. Les données à caractère non personnel peuvent être rangées dans deux catégories selon leur origine : la première catégorie a trait aux données qui ne concernent pas une personne physique identifiée ou identifiable, et la seconde catégorie a trait aux données qui, initialement étaient des données à caractère personnel, mais qui ont été ensuite rendues anonymes[470]. Les données anonymisées ne peuvent être attribuées à une personne donnée, même en utilisant des données supplémentaires, et sont donc des données à caractère non personnel[471]. Le Règlement (UE) 2018/1807 du Parlement européen et du Conseil du 14 novembre 2018 établissant un cadre applicable au libre flux des données à caractère non personnel dans l'Union européenne s'applique aux données à caractère personnel qui ont été correctement anonymisées.

Par ailleurs, des données à caractère personnel peuvent également se retrouver dans les informations publiques.

[470] Commission européenne, « Lignes directrices relatives au règlement concernant un cadre applicable au libre flux des données à caractère non personnel dans l'Union européenne », COM(2019) 250 final.
[471] *Ibid.*

B) Les données à caractère personnel et les données publiques

161. L'ouverture des données. L'ouverture des données publiques et la protection des individus sur leurs données à caractère personnel semblent au premier abord des objectifs antagonistes. En pratique, certains documents administratifs peuvent contenir des données à caractère personnel. Afin de ne pas freiner l'ouverture des données publiques, l'*open data* fait l'objet d'un encadrement législatif (1), encadrement qui s'efforce de trouver un équilibre entre ouverture et protection (2).

1. L'encadrement des données ouvertes

162. Contexte. La Loi n° 78-753 du 17 juillet 1978 dite « CADA » ne faisait aucune référence à la notion de données à caractère personnel. Pourtant, les informations publiques peuvent contenir des données à caractère personnel. Par la suite, la transposition de la Directive 2004/98/CE du Parlement européen et du Conseil du 17 novembre 2003 concernant la réutilisation des informations du secteur public par l'ordonnance n° 2005-650 du 6 juin 2005 relative à la liberté d'accès aux documents administratifs et à la réutilisation des informations publiques, la notion de données à caractère personnel a fait son apparition[472]. En opérant un changement de paradigme de l'accès à la possible réutilisation des données publiques, l'article 13 de l'ordonnance précitée prévoit que « la réutilisation d'informations publiques comportant des données à caractère personnel est subordonnée au respect des dispositions de la loi du 6 janvier 1978 susvisée, relative à l'informatique, aux fichiers et aux libertés ». Ensuite, lors de l'adoption de la loi pour une République numérique en 2016 et l'entrée en vigueur du RGPD en 2018, certaines règles sont venues modifier le principe d'ouverture des données publiques et à la protection des données personnelles[473]. Récemment, le Règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données (règlement sur la gouvernance des données) a également modifié les règles en matière de données publiques. Le règlement concerne certaines catégories de données protégées comme les données gardées fermées pour des raisons commerciales, de propriété intellectuelle ou encore les données à caractère personnel.

---

[472] Lanna Maximilien, « Données publiques et protection des données personnelles », Revue française d'administration publique, n° 167, École nationale d'administration, 2018.
[473] *Ibid*.

163. Principe. À titre principal, l'*open data* concerne les informations publiques et non les données à caractère personnel. Toutefois, certaines informations publiques sont susceptibles de contenir des données à caractère personnel. Afin de concilier les deux principes, l'article 6 de la loi pour une République numérique pose le principe suivant lequel « sauf dispositions législatives contraires ou si les personnes intéressées ont donné leur accord, lorsque les documents et les données mentionnés aux articles L. 312-1 ou L. 312-1-1 comportent des données à caractère personnel, ils ne peuvent être rendus publics qu'après avoir fait l'objet d'un traitement permettant de rendre impossible l'identification de ces personnes ». Selon ce principe, pour publier des documents administratifs contenant des données à caractère personnel, les administrations doivent procéder à un traitement pour anonymiser les documents[474]. En pratique, l'*open data* permet de croiser des informations publiques mises à disposition ou des données disponibles sur internet, ce qui permet d'identifier ou de réidentifier des personnes physiques. Dans ce cas, c'est bien l'usage de la donnée qui lui confère son caractère personnel[475]. Afin de protéger les personnes concernées, pour diffuser les documents contenants des données à caractère personnel, le principe reste l'anonymisation.

À la lecture de l'article L311-6 du CRPA, lorsque les données à caractère personnel relèvent de la vie privée des personnes concernées, les informations publiques ne peuvent être communiquées à des tiers, ni être publiées. Dès lors, ces informations ne sont communicables qu'à l'intéressé, elles sont dites « couvertes par le secret ». Le guide pratique de la CNIL et de la CADA « De la publication en ligne et de la réutilisation des données publiques ("*open data*") » donne une liste d'exemple des données relevant de la vie privée : « au titre de l'état civil, la date de la naissance et l'âge, les coordonnées personnelles, notamment l'adresse

[474] Article L.312-1-2 CRPA : « Sauf dispositions législatives ou réglementaires contraires, lorsque les documents et données mentionnés aux articles L. 312-1 ou L. 312-1-1 comportent des mentions entrant dans le champ d'application des articles L. 311-5 ou L. 311-6, ils ne peuvent être rendus publics qu'après avoir fait l'objet d'un traitement permettant d'occulter ces mentions. Sauf dispositions législatives contraires ou si les personnes intéressées ont donné leur accord, lorsque les documents et les données mentionnés aux articles L. 312-1 ou L. 312-1-1 comportent des données à caractère personnel, ils ne peuvent être rendus publics qu'après avoir fait l'objet d'un traitement permettant de rendre impossible l'identification de ces personnes. Une liste des catégories de documents pouvant être rendus publics sans avoir fait l'objet du traitement susmentionné est fixée par décret pris après avis motivé et publié de la Commission nationale de l'informatique et des libertés.
Les administrations mentionnées au premier alinéa de l'article L. 300-2 du présent code ne sont pas tenues de publier les archives publiques issues des opérations de sélection prévues aux articles L. 212-2 et L. 212-3du code du patrimoine. »

[475] Les collectivités territoriales et l'open data : concilier ouverture des données et protection des données personnelles, CNIL, 18 septembre 2019, disponible en ligne.

postale, l'adresse électronique et le numéro de téléphone, la situation patrimoniale et financière, en particulier le patrimoine immobilier, les revenus perçus, y compris les aides ou revenus de remplacement, les impôts et taxes acquittés, la domiciliation bancaire et l'identification des comptes bancaires et postaux mettent en cause la vie privée, la qualité de travailleur handicapé, la formation initiale, les horaires de travail, les sympathies politiques et l'appartenance à un parti politique ainsi que les croyances religieuses[476] ». La notion de « donnée privée » s'entend de manière stricte afin d'élargir le champ de l'*open data*[477].

164. Exceptions. Depuis l'entrée en vigueur du Règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données, les données protégées peuvent être réutilisées sous certaines conditions. Le règlement consacre son chapitre II à « La réutilisation de certaines catégories de données protégées détenues par des organismes du secteur public ». Le règlement propose donc un régime visant à concilier la protection et la réutilisation des données[478]. Ce dernier n'instaure pas un droit général de réutilisation des données protégées mais encadre les conditions de réutilisation : elles doivent être objectives, non discriminatoires, proportionnées et rendues publiques. Notamment, les mesures peuvent porter sur des obligations d'anonymisation, de pseudonymisation des données à caractère personnel ou de suppression des informations commerciales confidentielles[479]. Le règlement entend donc lever les restrictions qui font obstacle à la réutilisation des données publiques, même sensibles[480].

2. La recherche d'un équilibre entre ouverture et protection

165. Droit à l'information du public. Afin de promouvoir l'*open data*, le décret n°2018-1117 du 10 décembre 2018 liste les catégories de documents administratifs pouvant être rendus

[476] Commission nationale de l'informatique et des libertés et Commission d'accès aux documents administratifs, « Guide pratique de la publication et de la réutilisation des données publiques », 2016, p. 15.
[477] Cluzel-Métayer Lucie, « Les limites de l'open data », ADJA, 2016.
[478] Moussier Paul, « Les conséquences pour les personnes publiques du Data Governance Act », Revue internationale de droit des données et du numérique, 2023, pp. 57-72.
[479] Règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données (règlement sur la gouvernance des données), considérant 15.
[480] Cytermann Laurent, « L'ouverture des donnes publiques en Europe : principes et nouvelles frontières », *in* Bertrand Brunessen (dir.), *La politique européenne du numérique*, éd. Bruylant, 2023, p. 392.

publics sans faire l'objet d'un processus d'anonymisation[481]. En application de l'article 6 de la loi pour une République numérique, les documents dispensés d'anonymisation sont par exemple : les organigrammes et annuaires des administrations, le répertoire national des associations et le répertoire des entreprises et de leurs établissements dans leur intégralité, les annuaires des professions réglementées, les résultats obtenus par les candidats aux examens et concours administratifs ou conduisant à la délivrance des diplômes nationaux, les conditions d'organisation et d'exercice des activités sportives ; le répertoire national des élus, les registres des chambres d'hôtes et gîtes et pour finir la base des permis de construire[482].

L'application du présent décret permet d'établir un cadre assurant un juste équilibre entre la nécessaire information du public et la protection de la vie privée des personnes[483]. La liste n'est pas exhaustive et instaure des catégories de documents « nécessaires à l'information du public ». La notion d'« informations nécessaires au public » a été substituée à celle de « documents permettant au public d'être informé », notion trop générique. La Commission nationale de l'informatique et des libertés estime que « le dispositif réglementaire soumis pour avis à la commission ne devrait pas devenir le vecteur de publication par défaut des documents contenant des données à caractère personnel[484] ». Ainsi, l'anonymisation demeure la règle et la publication de documents administratifs comportant des données personnelles, l'exception.

166. Renforcement de la protection des individus. Les principes d'*open data* et de protection des individus sont des principes d'égale valeur. En réalité, la protection de la vie privée semble primer sur le principe de l'*open data.* Dans sa délibération, la CNIL ajoute des restrictions supplémentaires afin de renforcer la protection des individus : « enfin, la

[481] Décret n° 2018-1117 du 10 décembre 2018 relatif aux catégories de documents administratifs pouvant être rendus publics sans faire l'objet d'un processus d'anonymisation.

[482] Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique, article 6 : « Sauf dispositions législatives contraires ou si les personnes intéressées ont donné leur accord, lorsque les documents et les données mentionnés aux articles L. 312-1 ou L. 312-1-1 comportent des données à caractère personnel, ils ne peuvent être rendus publics qu'après avoir fait l'objet d'un traitement permettant de rendre impossible l'identification de ces personnes. Une liste des catégories de documents pouvant être rendus publics sans avoir fait l'objet du traitement susmentionné est fixée par décret pris après avis motivé et publié de la Commission nationale de l'informatique et des libertés. ».

[483] Lucchesi Laure, « Le décret fixant les catégories de données diffusables et réutilisables sans anonymisation est paru », Etalab.

[484] Délibération n° 2018-101 du 15 mars 2018 portant avis sur projet de décret pris pour l'application de l'article 6 de la loi n° 2016-1321 du 7 octobre 2016 pour une République numérique (demande d'avis n° 17001751).

commission rappelle que toute réutilisation des données à caractère personnel, notamment à des fins commerciales, devra être conciliée avec le droit d'opposition des personnes concernées. La réutilisation des données devra ainsi respecter la volonté des personnes concernées telle qu'exprimée lors de la collecte. Elle recommande ainsi aux administrations de mettre en œuvre des dispositifs permettant aux réutilisateurs d'identifier précisément les documents pour lesquels des droits d'opposition à certaines réutilisations ont été enregistrés par le responsable du traitement initial[485]. ». Le décret était censé faciliter la tâche aux administrations en leur permettant de diffuser des documents sans le consentement des personnes identifiées. Pourtant, la Commission nationale de l'informatique et des libertés évoque dans sa délibération le droit d'opposition des individus et écarte par-là certaines informations « nécessaires » à l'information du public. La Commission nationale de l'informatique et des libertés s'écarte de l'idée d'une conciliation équilibrée entre objectifs de même valeur pour faire prédominer l'un sur l'autre[486].

Ainsi, l'équilibre entre le principe d'*open data* et la protection des individus semble être atteint grâce au principe d'anonymisation. En réalité, ce principe comporte des faiblesses.

II. Les faiblesses de l'anonymisation

167. Anonymisation. En pratique, il existe plusieurs techniques d'anonymisation (1). Néanmoins, dans un contexte de *Big Data*, les risques de ré-identification démontrent les faiblesses des techniques d'anonymisation (2).

A) Le principe de l'anonymisation

168. Définitions et techniques. La notion d'anonymisation a été intégrée dans le droit dérivé afin de privilégier une protection étendue des personnes physiques sur leurs données (1). En pratique, il existe plusieurs techniques d'anonymisation (2).

485 Délibération, *op. cit*.

486 Maurel Lionel, « Open Data et protection des données personnelles », sur S.I.Lex, publié le 18 décembre 2018.

1. Notions d'anonymisation et de pseudonymisation

169. Notion de « pseudonymisation ». Tout d'abord, l'anonymisation ne doit pas être confondue avec la pseudonymisation. Afin de permettre une harmonisation maximale entre les États-membres de l'Union Européenne, le RGPD retient une définition unique de la « pseudonymisation ». L'article 4, point 5, énonce que la pseudonymisation est un « traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable ». Le règlement européen encourage l'utilisation de la pseudonymisation afin de réduire les risques pour les personnes concernées[487].

En pratique, la Commission nationale de l'informatique et des libertés précise que la pseudonymisation consiste à remplacer les données directement identifiantes (nom, prénom, etc) d'un jeu de données par des données indirectement identifiantes (alias, numéro séquentiel, etc)[488] : la pseudonymisation permet de traiter des données sans pouvoir les identifier directement. Toutefois, il est toujours possible de réidentifier les individus avec le croisement d'autres données. Ainsi, les données pseudonymisées demeurent des données à caractère personnel[489].

---

[487] *Ibid.,* considérant 28 : « La pseudonymisation des données à caractère personnel peut réduire les risques pour les personnes concernées et aider les responsables du traitement et les sous-traitants à remplir leurs obligations en matière de protection des données. L'introduction explicite de la pseudonymisation dans le présent règlement ne vise pas à exclure toute autre mesure de protection des données. ».

[488] Commission nationale de l'informatique et des libertés, « L'anonymisation de données personnelles », 19 mai 2020.

[489] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), considérant 26 : « Il y a lieu d'appliquer les principes relatifs à la protection des données à toute information concernant une personne physique identifiée ou identifiable. Les données à caractère personnel qui ont fait l'objet d'une pseudonymisation et qui pourraient être attribuées à une personne physique par le recours à des informations supplémentaires devraient être considérées comme des informations concernant une personne physique identifiable. ».

170. Notion d'anonymisation. Pour l'anonymisation, cette technique ne fait pas l'objet d'une définition propre dans les législations nationales ou européennes. L'analyse sémantique permet de faire le lien avec la notion « d'anonymat » qui représente « l'état de ce qui est anonyme », c'est-à-dire « ce dont on ignore le nom[490] ». Le suffixe renvoyant à l'anonymisation semble décrire le processus du changement d'état entre le connu et l'inconnu[491]. L'anonymisation est rendue possible par le recours au cryptage ou à l'effacement de certaines données. En 2020, la Commission nationale de l'informatique et des libertés partage ses lumières sur la notion et propose la définition suivante : « l'anonymisation est un traitement qui consiste à utiliser un ensemble de techniques de manière à rendre impossible, en pratique, toute identification de la personne par quelque moyen que ce soit et de manière irréversible[492] ». La notion d'« irréversible » est primordiale dans la mesure où cela sous-entend une obligation de résultat, les données ne doivent pas permettre de pouvoir identifier la personne physique.

171. Moyens raisonnables. Afin d'évaluer l'efficacité du processus et les possibilités de réidentification, le considérant 26 du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données évoque la prise en compte de « moyens raisonnablement susceptibles d'être utilisés » pour déterminer si une personne physique est identifiable. Pour évaluer le critère « raisonnable », il convient de prendre en compte « des facteurs objectifs, tels que le coût de l'identification et le temps nécessaire à celui-ci, en tenant compte des technologies disponibles au moment du traitement et de l'évolution de celles-ci ». Dans l'arrêt « Deloitte » du 26 avril 2023[493], le Tribunal considère - en s'appuyant sur la solution Breyer - que le caractère identifiable de l'information doit être analysé du point de vue de la personne qui détient l'information[494]. Ainsi, une même information pourra constituer une donnée à caractère personnel pour un acteur mais une donnée

[490] Dictionnaire de la langue française, Le Petit Robert, v° « Anonyme ».
[491] Eynard Jessica, *Les données personnelles ; quelle définition pour un régime de protection efficace ?,* éd. Michalon, 2013, p. 47.
[492] Commission nationale de l'informatique et des libertés, « L'anonymisation de données personnelles », 19 mai 2020.
[493] Tribunal de l'Union européenne, aff. T-557/20, Conseil de résolution unique (CRU) c/ Contrôleur européen de la protection des données (CEPD), 26 avril 2023.
[494] Lasserre Capdeville Jérôme, « Nouvel éclaircissement de la notion de données personnelles », Dalloz IP/IT, 2023, 540 ; CJUE, 19 oct. 2016, aff. C-582/14, Breyer, D., 2016, 2215.

anonymisée pour un autre[495]. L'analyse sera appréciée selon les moyens raisonnablement disponibles pour permettre la réidentification. Prenant en compte l'évolution des technologies, le règlement précité ne précise pas les techniques devant être utilisées[496].

172. Aspects essentiels. Pour le groupe G29, quatre aspects essentiels sont à retenir de cette notion. Tout d'abord, l'anonymisation peut être le résultat du traitement de données à caractère personnel dans le but d'empêcher irréversiblement l'identification de la personne concernée. En effet, plusieurs techniques d'anonymisation peuvent être envisagées et les éléments contextuels ont leur importance. Il faut prendre en considération « l'ensemble » des moyens « susceptibles » d'être « raisonnablement » utilisés à des fins d'indentification par le responsable de traitement ou par des tiers, en prêtant une attention particulière aux moyens que l'état actuel de la technologie a rendu récemment « susceptibles » d'être « raisonnablement » mis en œuvre. Enfin, pour apprécier la validité d'une technique d'anonymisation, il faut tenir compte du facteur de risque qui lui est inhérent - notamment des utilisations possibles des données « anonymisées » au moyen de cette technique - et évaluer la gravité et la probabilité de ce risque[497].

173. Différence entre l'anonymisation et la pseudonymisation. La différence entre anonymisation et pseudonymisation réside ainsi dans le caractère réversible ou non de la dissimulation des données à caractère personnel. Le Conseil d'État a eu l'occasion de rappeler cette indispensable nuance dans sa décision « JC Decaux ». Pour le Conseil d'État, s'il demeure possible d'individualiser une personne ou de relier entre elles des données résultant d'enregistrement qui la concerne, une donnée à caractère personnel ne peut pas être considérée comme rendue anonyme[498].

---

[495] Dubois Lorette, « Une nouvelle pierre à l'édifice de la notion de donnée à caractère personnel », Dalloz Actualité, 1er juin 2023.

[496] De Terwangne Cécile et Rosier Karen Rosier, *Le règlement général sur la protection des données. Analyse approfondie*, éd. Larcier, 2018, p. 65 : « Quant aux données anonymes, il est important de réaliser que l'anonymat d'aujourd'hui n'est pas d'office celui de demain et que cet anonymat doit être reconsidéré régulièrement au vu des développements techniques et des possibilités de croisement des données, notamment dans le cadre du Big Data, qui pourraient amener à un certain moment à réévaluer le caractère anonyme des données et à les faire rentrer dans la catégorie des données à caractère personnel. ».

[497] Groupe de travail de l'article 29 sur la protection des données, « Avis 05/2014 sur les techniques d'anonymisation », 10 avril 2014, p. 7.

[498] Conseil d'État, n° 393714, 8 février 2017 : point 7 : « En second lieu, il résulte de la définition de la donnée personnelle donnée par les dispositions, citées au point 2 ci-dessus, de l'article 2 de la loi du 6 janvier 1978, qu'une telle donnée ne peut être regardée comme rendue anonyme que lorsque l'identification de la personne

174. Exclusion du régime de protection. Lorsque l'anonymisation est effective, les données ne sont plus soumises aux obligations du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, n'étant plus considérées comme des données à caractère personnel[499]. Le RGPD n'impose aucune obligation d'anonymisation des données à caractère personnel, excepté pour la diffusion des documents par les administrations contenant des données à caractère personnel. L'anonymisation des documents est donc une obligation légale pour les administrations qui souhaitent diffuser les documents ou les données en ligne[500], sauf exceptions précitées. De surcroît, l'anonymisation est un véritable outil de confidentialité et de protection de la vie privée des individus[501]. L'appréciation se fera donc *in concreto* pour déterminer la qualification d'un jeu de données anonymes.

2. Les techniques d'anonymisation

175. Processus d'anonymisation. Avant d'utiliser toute technique d'anonymisation, la Commission nationale de l'informatique et des libertés recommande de prendre en compte des contraintes dès le début du projet : identifier les informations à conserver selon leur pertinence ; supprimer les éléments d'identification directe ainsi que les valeurs rares qui pourraient permettre un ré-identification aisée des personnes ; de distinguer les informations importantes des informations secondaires ou inutiles ; de définir la finesse idéale et acceptable pour chaque

concernée, directement ou indirectement, devient impossible que ce soit par le responsable du traitement ou par un tiers. Tel n'est pas le cas lorsqu'il demeure possible d'individualiser une personne ou de relier entre elles des données résultant de deux enregistrements qui la concernent. » ; « L'anonymisation d'une donnée doit rendre l'identification impossible », AJDA, 2017, 325.

[499] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), considérant 26 : « Il n'y a dès lors pas lieu d'appliquer les principes relatifs à la protection des données aux informations anonymes, à savoir les informations ne concernant pas une personne physique identifiée ou identifiable, ni aux données à caractère personnel rendues anonymes de telle manière que la personne concernée ne soit pas ou plus identifiable. Le présent règlement ne s'applique, par conséquent, pas au traitement de telles informations anonymes, y compris à des fins statistiques ou de recherche. ».

[500] Code des relations entre le public et l'administration, article L312-1-2.

[501] Tanghe Hélène et Gibert Paul-Olivier, « L'enjeu de l'anonymisation à l'heure du big data », Revue francaise des affaires sociales, 2017.

information conservée. Lorsque les contraintes sont identifiées et prises en compte, le responsable de traitement pourra déterminer la technique d'anonymisation à appliquer[502].

176. Fiabilité des techniques. La notion d'« anonymisation » est une notion interprétée de manière stricte. Au regard des recommandations du groupe G29, aucun seuil de ré-identification acceptable n'est envisagé. Le Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données tempère cette approche du risque zéro en renvoyant à des facteurs objectifs comme le coût, les technologies disponibles et leurs évolutions. En pratique, le texte sous-entendrait ici un raisonnement par le risque, avec une surveillance de ce risque dans le temps[503].

Afin de prendre en compte la fiabilité et l'adaptabilité de la technique, il convient d'analyser d'une part l'état de la technologie et, d'autre part, trois risques essentiels en matière d'anonymisation : « l'individualisation, à savoir l'impossibilité d'isoler un individu dans un ensemble de données ; la corrélation, à savoir l'impossibilité de relier entre eux des ensembles de données distincts concernant un même individu ; l'inférence, à savoir l'impossibilité de déduire une information sur un individu[504] ». Ainsi, pour être considérée comme fiable, la technique d'anonymisation devra résister aux trois risques de manière cumulative. En pratique, on distingue deux techniques d'anonymisation : la randomisation et la généralisation.

177. « Randomisation ». Selon l'avis du groupe de travail de l'article 29, la « *randomisation* » est une famille de techniques qui altèrent la véracité des données afin d'affaiblir le lien entre les données et l'individu[505]. Lorsque les données deviennent suffisamment incertaines, il n'est plus possible de les rattacher à un individu en particulier. Ces techniques sont aussi nommées « méthodes perturbatrices[506] » du fait d'altérer volontairement les données. Afin d'être efficace, le groupe de travail de l'article 29 préconise de combiner la randomisation à d'autres techniques comme l'ajout de bruit, la permutation ou la confidentialité

[502] Commission nationale de l'informatique et des libertés, « L'anonymisation de données personnelles », *op. cit.*
[503] Tanghe Hélène et Gibert Paul-Olivier, *op. cit*.
[504] *Ibid*.
[505] Groupe de travail de l'article 29 sur la protection des données (10 avril 2014). Avis 05/2014 sur les techniques d'anonymisation, p. 13.
[506] Tanghe Hélène et Gibert Paul-Olivier, *op. cit.*

différentielle. L'ajout de bruit consiste à modifier des attributs dans l'ensemble de données pour les rendre moins précis, tout en conservant la distribution générale. Il s'agit par exemple de modifier le poids ou la taille d'un individu à plus ou moins 5 kilogrammes ou cm. La permutation « consiste à mélanger les valeurs des attributs dans un tableau de telle sorte que certaines d'entre elles sont artificiellement liées à des personnes concernées différentes[507] ». Quant à la confidentialité différentielle, cela consiste à produire des aperçus de données anonymisées tout en conservant une copie des données originales. Cette technique permet d'indiquer au responsable du traitement des données quel niveau de bruit il doit ajouter, et sous quelle forme, pour obtenir les garanties nécessaires.

178. Généralisation. Au contraire de la randomisation, la généralisation est une « méthode non perturbatrice[508] ». La généralisation consiste à « généraliser, ou diluer, les attributs des personnes concernés en modifiant leur échelle ou leur ordre de grandeur respectif[509] ». Il s'agit de remplacer un mois par une année, une région plutôt qu'une ville, etc. Cette technique utilise les méthodes de « k-anonymisation », de « l-diversité » et de « t-proximité ». Le k-anonymat est une méthode qui empêche une personne d'être isolée en la regroupant avec au moins k autres individus. Il s'agit d'utiliser des valeurs d'intervalles ou des fourchettes de dates afin d'être moins précis. La l-diversité va plus loin en attribuant à chaque attribut au moins l valeurs différentes. Pour la t-proximité, cela « constitue un affinement de la l-diversité, en ce sens qu'elle vise à créer des classes d'équivalence qui ressemblent à la distribution initiale des attributs. Cette technique est utile quand il est important de conserver les données aussi proches que possible des données originales[510]. ».

Lorsque l'une des techniques ne résiste pas à l'un des trois risques d'appréciation de la fiabilité de la technique, il est nécessaire de prendre en compte les risques de ré-identification.

[507] Avis précité, p. 15.
[508] Tangue Hélène et Gibert Paul-Olivier, *op. cit*.
[509] Avis précité, p. 18.
[510] Avis précité, p. 20.

B) Les limites du principe d'anonymisation

179. Faiblesses. Dans un contexte de *Big Data*, les techniques d'anonymisation sont fragilisées par le risque de ré-identification (1), démontrant les faiblesses desdites techniques (2).

1. Le contexte de *Big Data*

180. Les risques de ré-identification. Les techniques d'anonymisation précitées ne sont pas exemptes de risques : à ce jour aucun dispositif d'anonymisation n'est infaillible. Dans la pratique, il existe un risque prégnant de réidentification, à une échelle différente selon la technique utilisée[511]. Les informaticiens le savent, l'anonymat est une notion obsolète : « toute donnée numérique - aussi impersonnelle, triviale, publique, anonyme soit-elle originairement - transpirant de nos actions et interactions en ligne et hors ligne est potentiellement susceptible de contribuer à nous (ré)identifier[512] ». En effet, les technologies évoluent et reposent sur des techniques de traitement permettant des corrélations poussées. Avec ces techniques, il est difficile voire impossible d'écarter tout risque de réidentification[513]. L'opposition des notions entre données à caractère personnel et données anonymes tend à s'estomper avec les diverses techniques de ré-identification[514].

181. Anonymisation et *Big Data*. Dans un contexte de *Big Data*, où le volume des données ne cesse de croître et les techniques d'analyse de s'améliorer, il devient de plus en plus simple d'obtenir de nouvelles informations[515]. En effet, d'aucuns considèrent que les capacités de

---

511 Narayanan Arvind et Felten Edward, « No silver bullet : De-identification still doesn't work », White Paper, 2014, p. 8 : « Change is difficult. When faced with the challenge of fostering data science while preventing privacy risks, the urge to preserve the status quo is understandable. However, this is incompatible with the reality of re-identification science. If a "best of both worlds" solution exists, deidentification is certainly not that solution. Instead of looking for a silver bullet, policy makers must confront hard choices. ».

512 Rouvroy Antoinette, « Homos juridicus soluble dans les données », *in* Cécile De Terwangne, Elise Degrave, Robert Queck, Séverine Dusollier (dir.), *Law, norms and freedoms in cyberspace. Droit, normes et libertés dans le cybermonde. Liber amicorum Yves Poullet*, éd. Larcier, 2018, p. 427.

513 Lequette Suzanne, *Droit du numérique*, éd. LGDJ, 2024, p. 689.

514 Rouvroy Antoinette, « Des données sans personne : le fétichisme de la donnée à caractère personnel à l'épreuve de l'idéologie des Big Data », 2014.

515 Poullet Yves, « Avant-propos : le RGPD - une volonté de bien faire : certes ! ... mais appropriée ? », *in* De Terwangne Cécile et Rosier Karen (dir.), *Le règlement général sur la protection des données (RGPD/GDPR), Analyse appronfondie, éd. Larcier,* 2018, p. 15 : « Une seconde remarque concerne le danger de ne s'attarder qu'aux données à caractère personnel et d'exclure les données dites anonymes dont l'utilisation est de plus en plus fréquente dans les réservoirs de données (les fameux Big Data). Non seulement, Il est loin

stockage et la puissance de calcul des ordinateurs ont fait « voler en éclat la notion d'anonymat[516] ». L'augmentation de la puissance de calcul des algorithmes et les nouvelles techniques de croisement de données permettent d'obtenir de nouvelles informations grâce à l'exploitation des d'autres sources d'informations disponibles[517]. À titre d'illustration, le « *data mining* » ou « exploration de données » permet l'extraction et l'analyse de données facilitant les corrélations entre les données : désormais, ce qui n'était pas à l'origine identifiant peut le devenir avec l'extraction et l'analyse de données. Avec le *Big Data*, l'agrégation des données est source de désanonymisation[518] : par conséquent, l'anonymisation est devenue illusoire[519].

2. Les limites des techniques

182. Fiabilité des résultats. Les techniques dites « perturbatrices » altèrent les données initiales afin de protéger les individus. Pour autant, selon le but recherché, les résultats peuvent être faussés en raison d'incohérences : « toute la difficulté réside dans le fait qu'en modifiant la véracité des données, l'exploitation des données est faussée, donnant lieu à des résultats d'analyse moins fiables[520] ». Selon le contexte, un résultat faussé peut avoir des conséquences sur les individus. Par exemple, un résultat moins fiable utilisé dans le contexte de la médecine peut entraîner des risques dans la décision de diagnostic d'un patient.

183. L'insuffisance des techniques. Deux illustrations fréquemment citées démontrent l'insuffisance des techniques d'anonymisation[521]. La première illustration concerne la société AOL, fournisseur d'accès à internet, qui avait publié en ligne une base de données, préalablement anonymisée, rassemblant 20 millions de recherches effectuées sur son site par

d'être évident que l'anonymat puisse résister à l'analyse massive et croisée de quantité de données mais en outre, combinées avec des données à caractère personnel, elles peuvent induire, dans des opérations de profilage, des discriminations non seulement individuelles mais également collectives. ».

516 Desmarais Pierre, « La réforme de l'open data suppose une approche globale », La Semaine Juridique Edition Générale, 2014.

517 Jommi Adel, « Le RGPD : un atout ou un frein pour la cybersécurité ? », Dalloz IP/IT, 2019, p. 352 : « Néanmoins, à l'heure du Big Data, de l'intelligence artificielle et du machine learning, une anonymisation ne garantit plus une protection infaillible car une réidentification est parfois possible par recoupement. ».

518 Castets-Renard Céline, « Les opportunités et risques pour les utilisateurs dans l'ouverture des données de santé », Revue Lamy Droit de l'Immatériel, n° spécial 108, 2014.

519 Douville Thibault, *Droit des données à caractère personnel,* éd. LGDJ, 2023, p. 135.

520 Tangue Hélène et Gibert Paul-Olivier, « L'enjeu de l'anonymisation à l'heure du big data », Revue française des affaires sociales, 2017.

521 Sénat, « La protection des données personnelles dans l'open data : une exigence et une opportunité », Rapport d'information.

650 000 utilisateurs sur trois mois. Les informations n'étaient pas directement identifiantes mais les liens entre les recherches d'un même utilisateur étaient conservés. Avec l'historique de recherche des internautes, il a été possible de retrouver l'identité de certains internautes grâce au croisement d'informations.

La seconde illustration concerne Netflix, qui avait publié quelque temps plus tard, un fichier contenant les recommandations de 50 000 utilisateurs, préalablement anonymisé aussi. Le fichier ne contenait pas d'information directement identifiante mais la note donnée par les utilisateurs à un film et sa date. À l'instar de la société AOL, des chercheurs en sécurité ont réussi à réidentifier plusieurs internautes « grâce au croisement de l'information donnée avec l'appréciation portée sur trois films, et la date à laquelle ils ont été loués, dès lors qu'ils avaient également publié des appréciations identiques aux mêmes dates, sur d'autres sites ou forums dans lesquels ils apparaissaient sous leur véritable identité[522] ».

Les exemples sont nombreux et sont directement liés à l'évolution des technologies. En pratique, il est même possible de se demander s'il existe encore des données à caractère non personnel[523]. Il serait désormais devenu « algorithmement impossible » de rester anonyme[524]. Les techniques d'analyse et le volume de données disponible permettent le croisement d'information, que ce soit à l'intérieur de la base de données ou grâce à d'autres informations disponibles. *In fine*, la protection des données à caractère personnel dépend des technologies disponibles et du coût investis dans la procédure d'identification[525].

[522] Tanghe Hélène et Gibert Paul-Olivier, *op. cit*.
[523] Perray Romain et Uzan-Naulin Julie, « Existe-t-il encore des données non personnelles ? », Dalloz IP/IT, 2017, p. 286.
[524] Basdevant Adrien et Mignard Jean-Pierre, *L'empire des données*, éd. Don Quichotte éditions, 2018.
[525] Strowel Alain, « Les données, un nouvel actif à l'intersection des propriétés intellectuelles », *in* Bruguière Jean-Michel, *La para-propriété intellectuelle*, éd. Dalloz, 2022, p. 111.

184. Conclusion de la section. L'instauration d'une typologie permet la répartition de régimes juridiques antagonistes, c'est-à-dire un régime d'ouverture ou un régime de protection des données. Les données à caractère personnel sont définies de manière extensive afin de protéger efficacement les utilisateurs contre les dérives d'usage des données à caractère personnel. Au contraire, la libre circulation des données à caractère non personnel et l'ouverture des données publiques sont devenues la norme.

Afin de maintenir cette dichotomie, les différentes législations permettent l'anonymisation des données. L'anonymisation permet de développer l'ouverture des données en échappant au régime protecteur des données à caractère personnel. En réalité, les technologies émergentes impactent la substance même du concept d'anonymisation. Avec la masse de données disponibles et les capacités d'analyse de plus en plus précises, les risques de ré-identification des données anonymisées sont prégnants.

Pourtant, l'anonymisation des données permet d'écarter le régime de protection des données à caractère personnel. *In fine*, le concept d'anonymisation rend incertain le champ de la notion des données à caractère personnel. À nouveau, les géants du numérique peuvent se servir de cette instabilité pour exploiter des données à caractère personnel artificiellement anonymisées.

Dès lors, la frontière entre les données à caractère personnel, les données à caractère non personnel et données publiques dépend de l'évolution des technologies. À ce jour, les frontières sont déjà poreuses et les technologies ne cessent d'évoluer. La typologie ne semble plus appropriée dans un contexte de *Big Data*. Ainsi, il serait nécessaire de prendre en compte l'usage des données, et particulièrement les usages des acteurs du numérique.

185. Conclusion du chapitre. La typologie des données repose sur une distinction selon la nature des données, la personne dont elles émanent ou leurs potentiels de réutilisation. Cette typologie permet d'établir des frontières entre les différentes données afin d'attribuer un régime juridique propre. Afin de s'adapter à l'environnement numérique, le législateur instaure peu à peu de nouvelles notions des données : les données d'intérêt général, les données de référence, les données à caractère personnel, les données à caractère non personnel, les données à forte valeur ajoutée, les données altruistes etc. Parfois, de nouveaux types de données comme les données de bien-être s'instaurent par la pratique. En réalité, la diversité des notions est évolutive et réduit parfois la primauté de la protection des données à caractère personnel dans une logique économique.

Pourtant, la typologie organise les frontières en fonction des risques ou du potentiel afin de leur attribuer un régime juridique propre. Néanmoins, l'usage des technologies émergentes entraîne des confusions entre les différentes données. Les données à caractère non personnel et les données à caractère personnel se retrouvent dans des ensembles de données mixtes et des données à caractère personnel dans les documents publics. Les technologies émergentes ne qualifient pas les données, elles en font usage.

À nouveau, l'instabilité de la typologie profite aux acteurs du numérique. Ils collectent et exploitent des masses de données sans se soucier des différentes frontières instaurées par le législateur. En pratique, la détermination des données en amont de leur traitement est un leurre pour les informaticiens. Les technologies émergentes renforcent l'instabilité de la typologie avec les jeux de données. *In fine*, malgré une définition théorique extensive des données à caractère personnel, l'instabilité permet de traiter ces données en toute opacité.

186. Conclusion du titre. L'étude sur la notion de donnée aboutit à des résultats contrastés. De manière positive, il faut prendre en compte l'évolution de la notion des données dans le cadre normatif. Pour développer le marché européen des données, le potentiel des données est renforcé par le développement de l'*open data* et la libre circulation des données à caractère non personnel. En parallèle, les données à caractère personnel sont définies de manière toujours plus extensive afin de protéger les individus sur l'exploitation de leurs données.

En réalité, la multiplication des notions de données constitue un risque pour la cohérence du cadre normatif. En effet, la polysémie entraîne des risques de confusion entre des notions voisines. Par ailleurs, l'usage des technologies émergentes fait naître des risques de chevauchement des différentes notions, la notion étant évolutive. Les notions ne sont pas classifiées dans les systèmes d'intelligence artificielle. L'absence de classification profite aux géants du numérique qui exploitent les données des utilisateurs.

La notion de donnée à caractère personnel s'avère artificiellement protectrice. Dès lors que l'anonymisation de ces données permet leur traitement, le champ de la notion de données à caractère personnel devient incertain. Avec le phénomène de *Big Data*, l'ensemble des données peuvent être réidentifiées grâce aux corrélations. Plus la masse de données est importante, plus les risques sont prégnants. Et à ce jour, ce sont les géants du numérique qui détiennent la majorité des données de la planète.

De façon pragmatique, l'excessive diversité de notions de données entraîne une excessive diversité de régimes juridiques applicables.

TITRE 2 : L'EXCESSIVE DIVERSITÉ DES NORMES

« Le droit contemporain est en crise. Il paraît incompréhensible. Les lois se succèdent à un rythme effréné semblant consacrer des droits contradictoires. Les directives suivies tirent le droit vers des extrêmes opposés. Les droits subjectifs se multiplient avec les droits fondamentaux tandis que l'économie de marché financiarisée ne cesse de tendre vers toujours plus de déréglementation. En parallèle, les sociétés multinationales créent leur propre droit, soft et global, et pèsent de tout leur poids pour faire basculer la balance de leur côté tant au sein des parlements nationaux et européens, par une intense activité de lobbying[526]*. »*

187. Remise en cause de la normativité traditionnelle. Les diverses notions de données sont soumises à des régimes juridiques différents. La construction des régimes juridiques soulève de nouveaux enjeux compte tenu de l'environnement numérique, par nature transfrontalier et virtuel. En effet, la normativité traditionnelle est mise à l'épreuve par les pratiques des géants du numérique qui agissent dans un cadre immatériel. Afin de s'adapter à ce nouvel environnement, l'Union européenne a adopté une politique propre au numérique.

L'ambition est de protéger les données à caractère personnel tout en libérant les flux de données à caractère non personnel : la mission pour le législateur européen est périlleuse au regard des objectifs diamétralement opposés. Il s'agit de garantir la protection des utilisateurs européens contre les pratiques des géants du numérique en parallèle du développement de l'ouverture des données en Europe. Ainsi, l'objectif est de construire un cadre normatif cohérent au sein d'un environnement global et complexe, actuellement dominé par des sociétés privées.

[526] Sintez Cyril, *Le droit construit : Penser le droit par le constructivisme*, éd. Dalloz, 2022, p. 209.

188. L'élaboration d'un marché unique numérique. Pour ce faire, la Commission Juncker a proposé dès 2015 une stratégie pour un marché unique numérique en Europe[527]. Le marché serait un espace dans lequel la libre circulation des biens, des personnes, des services et des capitaux est garantie. Un espace où les particuliers et les entreprises peuvent, quels que soient leur nationalité et leur lieu de résidence, accéder et se livrer à des activités en ligne et cela dans un cadre garantissant une concurrence loyale et un niveau élevé de protection des consommateurs et des données à caractère personnel. Ainsi, plusieurs normes vont émerger de cette stratégie tels que le règlement général sur la protection des données à caractère personnel[528], le règlement sur la cybersécurité[529], le règlement sur le libre flux des données à caractère non personnel[530] ou encore la directive sur les données ouvertes[531].

189. L'ambition d'un marché unique des données. En 2020, l'Union européenne va axer sa stratégie sur les données afin de « façonner l'avenir numérique de l'Europe[532] » en y intégrant un « espace européen des données[533] » voire un réel « marché unique des données[534] ». La stratégie de l'Union européenne est ubiquitaire tout en étant essentiellement axée sur le

---

527 Commission européenne, « Stratégie pour un marché unique numérique en Europe », COM(2015) 192 final.

528 Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

529 Règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications.

530 Règlement (UE) 2018/1807 du Parlement européen et du Conseil du 14 novembre 2018 établissant un cadre applicable au libre flux des données à caractère non personnel dans l'Union européenne.

531 Directive 2013/37/UE du Parlement européen et du Conseil du 26 juin 2013 modifiant la directive 2003/98/CE concernant la réutilisation des informations du secteur public. La directive a été abrogée par la directive (UE) 2019/1024 du Parlement européen et du Conseil du 20 juin 2019 concernant les données ouvertes et la réutilisation des informations du secteur public.

532 Commission européenne, « Façonner l'avenir numérique de l'Europe », Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions, COM(2020) 67 final.

533 *Ibid.*, p. 9 : « Les données sont devenues un facteur de production essentiel, et la valeur qu'elles créent doit être partagée avec l'ensemble de la société qui participe à la fourniture de ces données. C'est la raison pour laquelle nous devons construire un véritable marché unique européen des données : un espace européen des données fondé sur des règles et des valeurs européennes. ».

534 Commission européenne, « Une stratégie européenne pour les données », Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions, COM(2020) 66 final : « La stratégie européenne en matière de données doit permettre à l'Union européenne de devenir un acteur de premier plan dans une société axée sur les données. La création d'un marché unique des données permettra la libre circulation de ces dernières au sein de l'UE et entre les secteurs, dans l'intérêt des entreprises, des chercheurs et des administrations publiques. ».

potentiel de libéralisation des données. Afin de libérer les flux de données, il était nécessaire d'équilibrer les positions de monopoles des géants du numérique et de compléter les règles d'ouverture et de partage des données. À nouveau, plusieurs règlements vont entrer en vigueur tels que le Digital Service Act (DSA)[535], le Digital Market Act (DMA)[536], le Data Act (DA)[537], le Data Governance Act (DGA)[538] ou encore l'Intelligence Artificial Act (IA)[539]. *In fine*, le droit européen du numérique est devenu en quelques années une véritable « constellation normative[540] ».

190. Annonce de plan. La stratégie européenne sur les données repose sur la mise en place d'une réglementation ambivalente, prenant en compte à la fois la protection des données à caractère personnel et l'ouverture des données à caractère non personnel (**Chapitre 1**). De surcroît, il était nécessaire d'adapter les normes à la puissance des acteurs du numérique afin d'établir un équilibre sur le marché des données. Pour ce faire, une réglementation concurrentielle des données émerge (**Chapitre 2**).

[535] Règlement (UE) 2022/2065 du 19 octobre 2022 du Parlement européen et du Conseil relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (règlement sur les services numériques).
[536] Règlement (UE) 2022/1925 du Parlement européen et du Conseil du 14 septembre 2022 relatif aux marchés contestables et équitables dans le secteur numérique.
[537] Règlement (UE) 2023/2854 du Parlement européen et du Conseil du 13 décembre 2023 concernant des règles harmonisées portant sur l'équité de l'accès aux données et de l'utilisation des données (règlement sur les données).
[538] Règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données (règlement sur la gouvernance des données).
[539] Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle (règlement sur l'intelligence artificielle).
[540] Latil Arnaud, *Le droit du numérique. Une approche par les risques,* éd. Dalloz, 2023, p. 30.

Chapitre 1 : L'établissement d'un cadre ambivalent pour les données

191. Identification du régime juridique. Au regard de la pluralité des données, il n'existe pas un régime unique des données mais un régime juridique afférent à chaque catégorie de donnée. La nature de la donnée détermine son statut juridique et par conséquent son régime juridique. En pratique, les régimes applicables aux traitements des données sont dispersés à travers les différentes branches du droit. Selon la typologie des données, le régime juridique permet d'établir un cadre de protection ou, *a contrario*, un cadre d'ouverture des données.

192. Accumulation de régimes antagonistes. Afin de créer son espace unique européen des données, l'Union européenne mène une politique principalement d'ouverture des données. Pour autant, un équilibre doit être recherché entre la libre circulation et la protection des données à caractère personnel. L'équilibre s'avère quelque peu utopique face à la puissance des géants du numérique (**Section 1**). En revanche, les normes se sont multipliées afin d'essayer d'y parvenir. La multiplicité profite aux géants du numérique qui n'hésitent pas à intégrer dans les normes leurs propres intérêts. La prise en compte d'intérêts antagonistes affecte la cohérence du cadre normatif (**Section 2)**.

Section 1 : La recherche utopique d'un équilibre entre ouverture et protection des données

193. La protection des données à caractère personnel. Antérieurement à la stratégie européenne sur les données, la protection des données à caractère personnel avait déjà fait l'objet d'un pluralisme normatif important dans les années 1970. Dès 1978, la France va se doter d'un cadre juridique pour la protection des données à caractère personnel à la suite du scandale de l'affaire « SAFARI ». La Loi n° 78-17 du 6 janvier 1978 relative à l'informatique aux fichiers et aux libertés a édifié certains principes fondamentaux encore en vigueur à ce jour en matière de données à caractère personnel.

En 1995, le droit de l'Union européenne a complété le dispositif avec la 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. À partir des années 2000, les risques vont s'intensifier et changer de nature : les géants du numérique vont exploiter de manière abusive les données à caractère personnel des utilisateurs. Afin d'adapter la protection des données à caractère personnel à ces nouvelles pratiques, le Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données est entré en vigueur le 24 mai 2016 (I).

194. L'ouverture des données à caractère non personnel. En parallèle, l'ouverture des données à caractère non personnel représente un objectif économique pour l'Europe. Dans le dessein de contrer le monopole des géants du numérique sur les données à caractère personnel, l'Union européenne souhaite encourager le marché unique des données à caractère non personnel. Pour ce faire, ces données vont faire l'objet d'un régime antagoniste, c'est-à-dire un régime d'ouverture des données (II).

I. La protection des données à caractère personnel face à l'exploitation abusive

195. Annonce de plan. Dans un premier temps, afin de protéger effectivement les utilisateurs contre l'exploitation abusive de leurs données par les acteurs du numérique, un droit de la personnalité sur les données à caractère personnel a été consacré (A). Néanmoins, certains droits s'avèrent limités en pratique par la domination territoriale et logistique des géants du numérique (B).

A) La protection de la personne contre l'exploitation abusive

196. Analyse du statut de la donnée à caractère personnel. Le statut de la donnée à caractère personnel a fait l'objet de nombreux débats doctrinaux. L'analyse de ces débats permet de confirmer l'inopportunité d'une analyse patrimoniale (1) et de consacrer l'opportunité d'une analyse personnaliste pour les données à caractère personnel (2).

1. L'inopportunité de l'analyse patrimoniale

197. Absence d'argument juridique. L'opportunité d'une propriété a été émise par une partie de la doctrine au sujet des données à caractère personnel[541]. Au regard de la valeur des données, la donnée serait un bien sur lequel le droit reconnaîtrait un droit de propriété[542]. La propriété est définie par le célèbre article 544 du code civil qui dispose que « la propriété est le droit de jouir et de disposer des choses de la manière la plus absolue, pourvu qu'on n'en fasse pas un usage prohibé par les lois ou les règlements ». La propriété est un droit par nature absolu, perpétuel et qui confère à son titulaire le droit exclusif d'user (*usus*), de jouir (*fructus*) et de disposer (*abusus*) d'une chose. Les prérogatives de la Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés représenteraient selon cette doctrine l'appartenance et la maîtrise de ses données à caractère personnel pour les individus. Dès lors, la donnée devrait

[541] Anciaux Arnaud et Farchy Joëlle, « Données personnelles et droit de propriété », Revue internationale de droit économique, 2015 ; Peugeot Valérie, « Données personnelles : sortir des injonctions contradictoires », Vecam, avril 2014 ; Revet Thierry « La propriété de la personnalité », Gazette du Palais, 2007, n° 139 ; Bensoussan Alexandra « À terme, le droit de valoriser ses propres données apparaît inéluctable », RLDI, 2018 ; Hugentholtz Bernt « Propriété des données », Penser le droit de la pensée : mélanges en l'honneur de Michel Vivant, éd. Dalloz, 2020 ; Masson Florent, « Quel modèle "propriétaire" pour les données personnelles ? », RTD civ., octobre 2022, pp. 777-794.

[542] Rochfeld Judith, « Contre l'hypothèse de la qualification des données personnelles comme des biens », *in* Netter Emanuel (dir.), *Les biens numériques*, éd. CEPRISCA, p. 226.

être analysée comme un objet immatériel d'un droit de propriété[543]. Par le truchement de la propriété, la personne détiendrait un monopole sur ses données à caractère personnel, interdisant à tout tiers de tirer profit d'un tel bien sans aucune contrepartie financière[544].

En réalité, il nous semble que l'homme est possesseur de ses données et non propriétaire. La propriété doit être distinguée de la possession car la possession relève du fait et la propriété d'un pouvoir de droit. Les attributs de la possession étant l'*animus* (qui correspond à l'état d'esprit du possesseur) et le *corpus* (qui correspond au comportement du possesseur). Les attributs de la propriété ne sont pas exercés en totalité par l'homme puisqu'il peut faire un usage de ses données. Les fruits étant partagés - bien souvent de manière involontaire -, sans pour autant céder en totalité ses données[545]. La propriété revêt un caractère exclusif sur la donnée qui n'est pas réalisable en pratique puisque les données sont non-rivales : la non-rivalité des données rend par essence inadéquate tout régime de propriété[546] puisque la matérialité de l'objet suppose son unicité[547]. Par ailleurs, la consécration d'un droit de propriété sur les données à caractère personnel conduirait à identifier le responsable de traitement comme propriétaire. En pratique, ce sont majoritairement les géants du numérique qui exploitent les données à caractère personnel. L'instauration d'un droit de propriété reviendrait alors à rendre les GAFAM propriétaires de nos données à caractère personnel, ce qui n'est évidemment pas souhaitable, voire contreproductif au regard des objectifs européens.

198. Absence d'argument économique. Par-delà les arguments juridiques, la reconnaissance d'un droit de propriété sur les données à caractère personnel des utilisateurs n'emporterait aucun effet positif d'un point de vue économique. La donnée isolée n'a aucune valeur étant un bien non-rival et la valeur économique devient exponentielle lorsque les données sont croisées

[543] Catala Pierre, « La protection juridique des productions immatérielles », *in* Chamoux Jean-Pierre (dir.), *L'appropriation de l'information*, éd. Librairies techniques, 1986, p. 90 : « Aujourd'hui on admet d'une façon assez générale que l'information a une valeur intrinsèque, qu'elle a une valeur préexistante à son transfert, une valeur "capitaliste", une valeur en capital. Donc c'est un bien ! ».

[544] Boffa Romain, « La propriété des données personnelles », *in* Malabat Valérie et Zabalza Alexandre (dir.), *La propriété au 21ème siècle, un modèle ancestral toujours adapté aux grands enjeux de notre environnement ?,* éd. Dalloz, 2021, p. 110.

[545] Davadie Philippe, Kempf Olivier et Teboul Bruno, *La donnée n'est pas donnée*, éd. KAWA, 2016, p. 12.

[546] Pellegrini François, « La portabilité des données et des services », Revue française d'administration publique (RFAP), n° 167, École nationale d'administration, 2018.

[547] Poullet Yves, « La "propriété" des données. Balade aux "pays des merveilles" à l'heure du Big Data », *Penser le droit de la pensée : mélanges en l'honneur de Michel Vivant*, éd. Dalloz, 2020.

avec d'autres données[548]. À ce titre, le Conseil d'État corrobore cette analyse dans un rapport en rappelant l'absence de valeur de la donnée isolée et le renforcement potentiel des actes de collecte, de traitement et de croisement[549]. La rémunération d'un internaute pour ses données à caractère personnel relèverait seulement de quelques euros par an : la promesse de valorisation financière est illusoire[550]. En réalité, la rémunération de l'individu existe déjà par l'échange de la gratuité des services et de l'usage publicitaire des données[551].

Dans son rapport de 2014, le CNnum avance également l'argument selon lequel instaurer un droit de propriété ne ferait que renforcer les inégalités entre les citoyens en renvoyant à l'individu la responsabilité de gérer ses données[552]. La consécration d'un droit de propriété ne réduirait pas l'asymétrie de pouvoir informationnel entre l'utilisateur et le responsable de traitement[553]. Au contraire, les opérateurs pourraient profiter de cette situation en inscrivant des clauses de cession obligatoire dans les contrats, aboutissant à un risque de dépossession inévitable pour les individus[554]. *In fine*, l'officialisation d'une dimension économique des données à caractère personnel pourrait finir par se retourner contre les individus censés être protégés. L'ensemble des citoyens ne serait plus protégé de manière équilibrée et le droit des données à caractère personnel deviendrait un droit ésotérique[555]. Ainsi, l'instauration d'un droit de propriété profiterait spécifiquement aux géants du numérique et non aux utilisateurs.

---

548 Bertrand Brunessen, « La gouvernance des données dans la régulation européenne de l'intelligence artificielle », RTDE, n°3, 2022, pp. 315-331.

549 Conseil d'État, « Le numérique et les droits fondamentaux », La Documentation française, 2014, p. 266 : « Le rééquilibrage de la relation entre les éditeurs de services numériques et les internautes, qui découlerait de la reconnaissance d'un tel droit de propriété, apparaît largement illusoire. […] Même si le prix des données de chaque individu est appelé à croître de manière considérable au cours des années à venir (jusqu'à quelques euros), la valeur de l'actif que la reconnaissance du droit de propriété conférerait à chaque individu restera dérisoire. Les acteurs du numérique rédigeraient leurs contrats comme la fourniture d'un service en échange de la cession de droits d'utilisation des données, ce dont nombre de conditions générales d'utilisation se rapprochent déjà beaucoup ; le rapport de forces entre l'individu, consommateur isolé et l'entreprise, resterait marqué par un déséquilibre structurel. ».

550 Anciaux Arnaud et Farchy Joëlle, *op. cit*.

551 Benabou Valérie-Laure et Rochfled Judith, *À qui profite le clic ?*, éd. Odile Jacob, 2015, p. 27.

552 CNnum, « Neutralité des plateformes : réunir les conditions d'un environnement numérique ouvert et soutenable », Rapport, Conseil National du Numérique, Paris, mai 2014, p. 37.

553 Ochoa Nicolas, « Pour en finir avec l'idée d'un droit de propriété sur ses données personnelles : ce que cache véritablement le principe de libre disposition », RDFA, 2015, p. 1157 : « Une telle asymétrie s'explique par le caractère technique et complexe du droit des données personnelles. ».

554 Poullet Yves, « Consent : "The privacy bug" », La confiance numérique, travaux de la Chaire sur la confiance numérique, LexisNexis, Paris, p. 98 : « La "vie privée" deviendrait un privilège de nantis. ».

555 Revet Thierry, « Les données, nouveau(x) bien(s) ? », *in* Bruguière Jean-Michel, *L'émergence d'un droit des données*, éd. Dalloz, 2023.

199. Tempéraments. Il existe toutefois certains tempéraments au refus de l'analyse patrimoniale. Le code de la propriété intellectuelle consacre un régime de protection pour les bases de données. Les bases de données sont définies comme « un recueil d'œuvres, de données ou d'autres éléments indépendants, disposés de manière systématique ou méthodique, et individuellement accessibles par des moyens électroniques ou par tout autre moyen[556] ». Ces dernières peuvent faire l'objet d'une double protection : par le droit d'auteur sous réserve d'originalité et par le droit *sui generis* lorsque la constitution de la base de données « atteste d'un investissement financier, matériel ou humain substantiel[557] ». Néanmoins, cette protection sert à couvrir un investissement substantiel du producteur de la base de données et non les données brutes[558]. Dans l'hypothèse où la base de données est composée uniquement de données à caractère personnel, elle est soumise au régime protecteur du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

Ainsi, selon le droit positif, l'individu n'est pas propriétaire de ses données à caractère personnel. En revanche, l'analyse personnaliste apparait plus opportune au regard des objectifs du régime juridique de la protection des données à caractère personnel.

2. L'opportune consécration de l'analyse personnaliste

200. Un droit de la personnalité. Le rapport d'un individu à ses données à caractère personnel est un rapport à sa propre personne[559]. Les informations relatives à l'individu reflètent sa personnalité, son identité[560]. D'un point de vue étymologique, le terme « personne » provient du latin « *persona* », désignant un masque de théâtre. L'origine de ce terme permet de

[556] Directive 96/9/CE du Parlement européen et du Conseil, du 11 mars 1996, concernant la protection juridique des bases de données ; Code de la propriété intellectuelle (CPI), article L112-3.

[557] Code de la propriété intellectuelle (CPI), article L341-1 : « Le producteur d'une base de données, entendu comme la personne qui prend l'initiative et le risque des investissements correspondants, bénéficie d'une protection du contenu de la base lorsque la constitution, la vérification ou la présentation de celui-ci atteste d'un investissement financier, matériel ou humain substantiel. Cette protection est indépendante et s'exerce sans préjudice de celles résultant du droit d'auteur ou d'un autre droit sur la base de données ou un de ses éléments constitutifs. ».

[558] CNnum, « La libre circulation des données dans l'Union Européenne », avis, avril 2017.

[559] Viangalli François, « Le concept de données en droit du numérique. Essai de définition », Revue Lamy Droit de l'Immatériel, n° 202, 1er avril 2023.

[560] Rochfled Judith, *Les grandes notions du droit privé,* éd. PUF, 2022, p. 99.

comprendre que la personnalité est avant tout un rôle social. Dans l'environnement numérique, l'identité numérique devient une composante de la personnalité de l'individu. Les droits de la personnalité ayant essentiellement une vocation défensive, la personne va pouvoir défendre son identité numérique[561] : la protection devient alors une prérogative de la personne, c'est-à-dire un droit de la personnalité[562]. Par conséquent, les données à caractère personnel sont considérées comme des informations relatives à une personne physique et non comme des biens, au regard de leur caractère indétachable de l'être humain[563]. La donnée est protégée en tant qu'élément d'identification d'une personne physique et non en tant que chose ; l'exclusion des personnes morales renforce par ailleurs l'analyse personnaliste[564]. Ainsi, les données à caractère personnel deviennent un attribut de la personnalité et par conséquent, un élément incessible. La consécration de l'analyse personnaliste permet d'assurer à l'individu une protection fondamentale de ses données à caractère personnel.

201. Un droit fondamental. En effet, le régime juridique des données à caractère personnel a été instauré pour permettre aux utilisateurs de protéger leurs libertés fondamentales[565]. Au début des années 1970, l'insuffisance de protection de l'article 8 de la Convention de sauvegarde des droits et libertés fondamentaux - garantissant le droit à la vie privée et familiale pour protéger les données à caractère personnel des individus - a été relevée au regard du développement des technologies émergentes[566]. Afin de contrer cette insuffisance, le droit à la protection des données à caractère personnel a été promu tel un droit quasi-constitutionnel par l'adoption à la fois de l'article 8 de la Charte des droits fondamentaux de l'Union Européenne et de l'article

---

561 Netter Emmanuel, *Numérique et grandes notions du droit privé*, éd. CEPRISCA, 2019, p. 42 : « Entre les traits véritables de l'acteur et le regard du public, le masque s'interpose. Il occulte une réalité et en impose une autre. Et en effet, à travers la notion de "personne", ce n'est pas la réalité profonde de l'être humain que l'on cherche à saisir, mais seulement sa projection publique. Le droit ne se mêle pas de la vie intérieure, mais il s'impose dans l'existence sociale. ».

562 Mallet-Poujol Nathalie, « Appropriation de l'information : l'éternelle chimère », Recueil Dalloz, 1997, 38, p. 330.

563 Frison-Roche Marie-Anne, « Le Droit de la Compliance relatif aux "données" », disponible en ligne.

564 Boffa Romain, *op. cit.*, p.110.

565 Gutwirth Serge et Gonzalez Fuster Gloria, « L'éternel retour de la propriété des données : de l'insistance d'un mot d'ordre », *in* De Terwangne Cécile, Degrave Elise, Queck Robert et Dusollier Séverine (dir.), *Law, norms and freedoms in cyberspace. Droit, normes et libertés dans le cybermonde. Liber amicorum Yves Poullet*, éd. Larcier, 2018, pp. 117-140.

566 Ailincai Mihaela Anca, « Différents standards européens de protection des données ? À propos du droit de l'Union européenne et du droit du Conseil de l'Europe », *in* Bensamoun Alexandra et Bertrand Brunessen (dir.), *Le règlement général sur la protection des données, Aspects institutionnels et matériels,* éd. Mare & Martin, 2020, p.101.

16, paragraphe 1er du Traité sur le fonctionnement de l'Union Européenne[567]. De ce fait, le droit à la protection des données à caractère personnel devient autonome au droit de la protection de la vie privée[568].

Ainsi, un véritable écosystème du droit à la protection des données à caractère personnel s'est construit à partir de droits fondamentaux, permettant à l'individu de garder *a priori* le contrôle sur ses données[569].

202. Droit à l'autonomie informationnelle. Le contrôle de l'individu sur ses données est symbolisé par le droit à l'autonomie informationnelle[570]. Cette prérogative n'est pas un droit supplémentaire pour les individus[571] mais se « situe à un autre niveau : il donne sens à tous ces droits, qui tendent à le garantir et doivent être interprétés et mis en œuvre à la lumière de cette finalité »[572]. Le droit à l'autonomie informationnelle a été inspiré par un arrêt de la Cour constitutionnelle fédérale allemande se basant sur l'article 1er (dignité humaine) et l'article 2 (développement de la personnalité) de la Constitution pour sa consécration[573]. En pratique, le

---

567 Charte des droits fondamentaux de l'Union Européenne, article 8.1 : « Toute personne a droit à la protection des données à caractère personnel la concernant ». La Charte des droits fondamentaux est dotée d'une portée juridique identique à celle des traités depuis l'entrée en vigueur du traité de Lisbonne, le 1er décembre 2009 ; Traité sur le fonctionnement de l'Union européenne, article 16 : «. 1. Toute personne a droit à la protection des données à caractère personnel la concernant. ». Cet article accroit la responsabilité de l'Union Européenne de respecter ce droit. L'article 16, paragraphe 2, dudit traité donne mandat au Parlement européen et au Conseil pour fixer les règles relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel ainsi que les règles relatives à la libre circulation des données à caractère personnel.

568 En tant que gardienne de ce droit, la CJUE veille à rappeler cette fondamentalité dans ses décisions (« le droit fondamental qui garantit la protection des données à caractère personnel », CJCE, 29 janvier 2008, Promusicae, n° C-275/06).

569 Tinière Romain, « Les données personnelles, source de nouveaux droits fondamentaux ? », *in* Bruguière Jean-Michel, *L'émergence d'un droit des données*, éd. Dalloz, 2023, pp. 55-65.

570 Poullet Yves, « 50 ans de législations européennes de protection des données. Hier, aujourd'hui et demain. », *in* Bévière-Boyer Bénédicte, Dibie Dorothée et Arlotti Clément (dir.), *Numérique, droit et société*, éd. Dalloz, 2022, p. 25.

571 Martial-Braz Nathalie, « Le renforcement des droits de la personne concernée », Dalloz IP/IT, 2017, p. 253.

572 Conseil d'État, *op. cit*., p. 267.

573 Cour constitutionnelle fédérale allemande, 15 décembre 1983 : Il ressort des motifs de la décision un triple fondement : « la liberté de la personne à exercer la plénitude de ses droits, sans contrainte, menace, ni pression ; l'autonomie de la personne, dont le libre épanouissement, le développement personnel serait entravé par des traitements de données personnelles abusifs ; la dignité humaine, face au risque d'une société fondée sur la surveillance généralisée, où l'être humain ne serait plus sujet mais objet », 15 Décembre 1983.

droit à l'autodétermination doit guider toute révision des régimes de protection des données[574]. En réalité, le Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ne reconnaît pas en tant que tel le droit à l'autodétermination informationnelle. Toutefois, au niveau national, l'article 1er de la Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés symbolise l'esprit de ce droit en disposant que « toute personne dispose du droit de décider et de contrôler les usages qui sont faits des données à caractère personnel la concernant[575] ».

Face aux pratiques d'exploitation des données à caractère personnel des utilisateurs, il était fondamental de consacrer une approche personnaliste : les individus doivent être protégés par le droit contre les pratiques immorales des sociétés privées. En réalité, malgré l'institution d'un droit quasi-constitutionnel de la protection des données à caractère personnel, certaines prérogatives accordées aux individus sont limitées en pratique.

B) Les faiblesses de certains droits face à l'exploitation abusive

203. Limites des droits subjectifs. Afin d'exercer leur autodétermination informationnelle, les individus disposent de prérogatives issues du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données : le droit à l'effacement et le droit à la portabilité font partie des droits subjectifs reconnus aux utilisateurs afin de garder le contrôle sur leurs données. En pratique, le droit à l'effacement est restreint territorialement (1) et le droit à la portabilité est quant à lui, limité par certaines contraintes techniques (2).

[574] Rouvroy Antoinette, « Le droit à l'autodétermination informationnelle et la valeur du développement personnel : une réévaluation de l'importance du droit à la protection de la vie privée pour la démocratie », État de droit et virtualité, Thémis, Montréal, p. 157-222.
[575] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, dit loi informatique et libertés.

1. Les restrictions territoriales du droit à l'effacement

204. Principe du droit à l'effacement (« droit à l'oubli »). En apparence, le droit à l'effacement permet à chaque individu de contrôler l'avenir de ses données à caractère personnel sur l'environnement numérique. En effet, cet environnement atypique ne dispose pas d'un « oubli naturel » mais bien au contraire, d'une mémoire intemporelle[576]. Afin de permettre aux individus d'effacer des informations accessibles au public le concernant, la Cour européenne a consacré en 2014 dans l'arrêt « Google Spain » un droit à l'effacement[577]. De façon louable, il est précisé que les droits de la personne doivent prévaloir sur l'intérêt économique de l'exploitant du moteur de recherche[578]. Le Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel a renforcé ce droit. Le règlement précise que tout individu a le droit de demander au responsable de traitement l'effacement de ses données à caractère personnel[579]. Le droit à l'effacement serait donc une alternative pour les individus afin d'effacer les données qu'ils souhaitent se réapproprier.

205. Un droit restreint. En pratique, la portée de ce droit est bien plus restreinte que son existence médiatique[580] : peu d'utilisateurs sollicitent l'effacement de leurs données à caractère personnel. Par ailleurs, le droit à l'effacement est conditionné à certains motifs tels que lorsque les données ne sont plus nécessaires au regard de la finalité du traitement, lorsque la base légale (consentement) est tombée, lorsque le droit d'opposition a été exercé de manière fructueuse,

---

[576] Rochfled Judith, « "Droit à l'oubli numérique" et construction de soi : peut-on se faire oublier sur les réseaux numériques ? », *in* Parat Hélène, Angelergues Jacques et Cointot Françoise (dir.), *Mémoires : se souvenir, oublier,* éd. PUF, 2021, p. 86 : « La documentation intégrale des identités prive les individus comme les collectifs d'une fonction essentielle : celle d'organiser le mémorable. L'enregistrement s'effectuant par défaut, c'est désormais l'effacement des traces et non leur conservation qui exige volontarisme, dépense et savoir-faire. Après avoir réclamé un devoir de mémoire, les sociétés modernes se préoccupent donc aujourd'hui d'un droit à l'oubli. » (Merzeau, 2013, nº 59).

[577] Cour de Justice de l'Union européenne (CJUE), 13 mai 2014, aff. C-131/12, Google Spain SL et Google Inc. c/ Agencia Espanola de Proteccion de Datos et Gonzales.

[578] *Ibid.*, point 97.

[579] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), article 17 : « La personne concernée a le droit d'obtenir du responsable du traitement l'effacement, dans les meilleurs délais, de données à caractère personnel la concernant et le responsable du traitement a l'obligation d'effacer ces données à caractère personnel dans les meilleurs délais. ».

[580] Martial-Braz Nathalie, « Le droit au déréférencement : vraie reconnaissance et faux-semblants », Dalloz IP/IT, 2019, p. 631.

lorsque les données ont été traitées de manière illicite ou encore lorsque les données concernent un mineur. Finalement, les utilisateurs ne peuvent pas simplement solliciter le droit à l'effacement lorsqu'ils décident de se réapproprier leurs données à caractère personnel. Il s'agit d'un droit encadré et restreint puisqu'il s'agit uniquement de permettre l'effacement de traitements non licites[581]. Ainsi, la portée du droit à l'effacement s'avère restreinte lorsque les traitements sont licites.

206. Un droit relatif. En outre, le droit à l'effacement doit être concilié avec la liberté d'expression ou le droit à l'information[582]. Pour ce faire, le Conseil d'État a élaboré un « guide » dans l'intention d'éclairer les responsables de traitement. Selon la juridiction suprême de l'ordre administrative seules trois catégories de données à caractère personnel sont concernées par le droit au déréférencement : les données à caractère personnel qui ne relèvent pas de catégories particulières, les données à caractère personnel dites « sensibles » et les données à caractère personnel dites « pénales ». Pour les données sensibles et pénales, le refus à l'effacement ne peut être légalement justifié uniquement si l'accès à ces données à partir d'une recherche portant sur le nom du demandeur est strictement nécessaire à l'information du public. En revanche, pour les données touchant à la vie privée sans être sensibles, le refus peut être justifié sur l'intérêt au public d'accéder à l'information en cause[583]. Les individus peuvent donc se voir refuser une demande d'effacement au motif d'un droit à l'information prépondérant. La notion pouvant être interprété de manière large et ne bénéficiant nécessairement pas aux individus concernés.

207. Un droit limité. Par ailleurs, le droit à l'effacement n'a pas de portée internationale. La Commission nationale de l'informatique et des libertés avait honorablement subordonné l'effectivité de ce droit à sa portée géographique. Selon la Commission nationale de l'informatique et des libertés, « seule une mesure s'appliquant à l'intégralité du traitement lié au moteur de recherche, sans distinction entre les extensions interrogées et l'origine

581 Castets-Renard Céline, « Brève analyse du règlement général relatif à la protection des données personnelles », Dalloz IP/IT, 2016, p. 331.

582 Cour européenne des droits de l'homme, n° 60798/10 et n° 65599/10, 28 juin 2018.

583 Conseil d'État, « Droit à l'oubli : le Conseil d'État donne le mode d'emploi », 6 décembre 2019 : « Par 13 arrêts du 6 décembre 2019, le Conseil d'État fixe les conditions dans lesquelles doit être respecté le droit au déréférencement sur internet prévu par le RGPD. Il est ainsi la première juridiction française à livrer, à Google et à la Commission nationale de l'informatique et des libertés (CNIL), un mode d'emploi du droit de l'oubli. ».

géographique de l'internaute effectuant une recherche est juridiquement à même de répondre à l'exigence de protection[584] ». Malgré cette recommandation, la Cour de Justice de l'Union européenne a déterminé qu'il n'existe aucune obligation de procéder au déréférencement sur l'ensemble des moteurs de recherche[585]. Conformément à cette décision, le Conseil d'État a annulé une décision de la Commission nationale de l'informatique et des libertés exigeant un déréférencement applicable à l'ensemble du traitement, c'est-à-dire à l'échelle mondiale[586]. La Haute juridiction administrative rappelle qu'aucune disposition législative ne permet à un déréférencement « d'excéder le champ couvert par le droit de l'Union européenne »[587]. Pourtant, la limitation territoriale du droit à l'effacement à l'Union européenne a pour effet d'anéantir en partie la portée de ce droit : les données seront toujours accessibles lorsque les recherches seront effectuées à partir d'un nom de domaine avec une extension non européenne[588]. La restriction du droit à l'effacement aux frontières européennes nous semble contreproductive au regard de l'espace numérique[589]. Les utilisateurs souhaitant exercer leur droit au déréférencement seront désenchantés face à la publicité faite de ce droit[590].

Par-delà cette possibilité d'effacer ses données à caractère personnel dans l'environnement numérique, cela ne permet pas pour autant leur réappropriation. Ainsi, le règlement sur la protection des données instaure un droit à la portabilité.

---

584 Commission nationale de l'informatique et des libertés, 10 mars 2016, délibération n° 2016-054.

585 Cour de Justice de l'Union européenne, aff. C-507/17, 24 septembre 2019, point 64 : « Il s'ensuit que, en l'état actuel, il n'existe, pour l'exploitant d'un moteur de recherche qui fait droit à une demande de déréférencement formulée par la personne concernée, le cas échéant, à la suite d'une injonction d'une autorité de contrôle ou d'une autorité judiciaire d'un État membre, pas d'obligation découlant du droit de l'Union de procéder à un tel déréférencement sur l'ensemble des versions de son moteur. ».

586 Conseil d'État, 27 mars 2020, n° 399922, publié au recueil Lebon.

587 *Ibid.*, point 10 : « Si la CNIL soutient en défense que la sanction contestée trouve son fondement dans la faculté que la Cour de justice a reconnue aux autorités de contrôle d'ordonner de procéder à un déréférencement portant sur l'ensemble des versions d'un moteur de recherche, il ne résulte, en l'état du droit applicable, d'aucune disposition législative qu'un tel déréférencement pourrait excéder le champ couvert par le droit de l'Union européenne pour s'appliquer hors du territoire des États membres de l'Union européenne. ».

588 Benabou Valérie-Laure, « Une cinquième liberté de circulation numérique ? Est-ce possible ? Est-ce utile ? », RTD eur., 2021, p. 287.

589 Netter Emmanuel, « Le modèle européen de protection des données personnelles à l'heure de la gloire et des périls », *in* Netter Emmanuel (dir.), *Regards sur le nouveau droit des données personnelles*, éd. CEPRISA, 2019, p. 29.

590 Poullet Yves, « Cinq ans après – le RGPD est-il toujours la solution ? », RDTI, n° 90, 2023, p. 16 : « On ajoutera les difficultés pour la personne concernée de pouvoir exercer pleinement son droit à l'oubli. ».

2. Les limites techniques du droit à la portabilité

208. Principe du droit à la portabilité. Dès 2012, l'instauration d'un droit à la portabilité a été sollicitée par la Commission européenne lors des discussions sur la réforme des données à caractère personnel[591]. L'intégration de ce droit dans le règlement sur la protection des données à caractère personnel a été considérée comme une innovation.[592] À l'instar du droit à l'oubli, le droit à la portabilité est une manifestation du principe d'autodétermination informationnelle[593]. En effet, le droit à la portabilité permet de renforcer la maîtrise des utilisateurs sur leurs données[594], voire de constituer un véritable outil d' « *empowerment* » pour eux[595]. Les utilisateurs peuvent récupérer leurs données collectées par un responsable de traitement afin de les transférer à un tiers ou de les réutiliser de façon personnelle. Pour les responsables de traitement, le droit à la portabilité permet de favoriser la concurrence entre les services en ligne. L'aspiration de ce droit est effectivement de réguler la concurrence en permettant aux utilisateurs de changer de fournisseur de service sans perdre leurs données.

209. Un droit limité aux données « fournies ». Pour autant, le droit à la portabilité ne s'applique qu'aux données « fournies » par la personne concernée. Dès lors, les autorités de contrôle recommandent une interprétation extensive de la notion de données « fournies » : il s'agit des données « déclarées activement et consciemment par la personne concernée » mais également des données « générées par l'activité de la personne concernée », c'est-à-dire notamment ses traces ou ses historiques de navigation[596]. L'interprétation extensive était indispensable puisqu'une grande partie des données collectées et exploitées par les GAFAM sont des données générées inconsciemment par les individus ; une interprétation restrictive aurait réduit la portée du droit à la portabilité aux données fournies activement, soit une faible

[591] Commission européenne, « La Commission propose une réforme globale des règles en matière de protection des données pour accroître la maîtrise que les utilisateurs ont sur leurs données, et réduire les coûts grevant les entreprises », Communiqué de presse, IP/12/46, 25 janvier 2012.

[592] Metallinos Nathalie, « La protection des données au service de l'émancipation du consommateur », CCE, 2017, 17.

[593] Zolynski Célia et Le Roy Marylou, « La portabilité des données personnelles et non personnelles, ou comment penser une stratégie européenne de la donnée », Légicom, Revue du droit de la communication des entreprises et de la communication publique, 2017, 59, p. 105.

[594] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), article 20.

[595] Anciaux Nicolas et Zolynski Célia, « Empowerment et Big Data sur données personnelles. De la portabilité à l'agentivité », *in* G'Sell Florence (dir.), *Le Big Data et le Droit*, éd. Dalloz, 2020.

[596] Groupe 29, « Lignes directrices relatives au droit à la portabilité des données », 16/FR, WP 242.

partie des données exploitées. Néanmoins, les données « dérivées », c'est-à-dire des données manipulées par le responsable de traitement afin d'en extraire une valeur ajoutée, ne font pas partie des données concernées par le droit à la portabilité. Malheureusement, les acteurs du numérique pourront inclure une partie des données dans cette catégorie afin de ne pas appliquer cette prérogative.

210. Des difficultés techniques. En pratique, la mise en œuvre du droit à la portabilité doit se faire dans un « format structuré, couramment utilisé et lisible par machine[597] ». Les responsables de traitement vont devoir anticiper les demandes des utilisateurs et utiliser des formats interopérables. En réalité, les formats sont rarement suffisamment interopérables. L'insuffisance technique vide de sa substance le principe de portabilité des données[598]. Pour autant, les responsables de traitement sont dans l'obligation d'intégrer ce droit dans la cartographie de leurs traitements afin d'éviter un traitement manuel des demandes[599]. Ainsi, il revient aux responsables de traitement d'anticiper la portabilité des données dans le traitement des données.

211. Une charge financière importante. Pour les petites entreprises ou les entreprises non-spécialistes du numérique, l'anticipation et l'exécution du droit à la portabilité constituent une charge financière conséquente. Les responsables de traitements doivent recourir à des standards et des formats interopérables : le processus est long et coûteux. La charge financière de cette obligation peut alors constituer une barrière à l'effectivité de ce droit. Les responsables de traitement sont rarement des juristes et peuvent rencontrer des difficultés à anticiper le droit à la portabilité. Pour le moment, ce droit est difficilement compris par les responsables de traitement[600]. En réalité, une faible partie des acteurs du numérique sera en en mesure d'appliquer concrètement cette mesure et cela s'avère préjudiciable pour les utilisateurs[601].

---

[597] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 précité, article 20 : « Les personnes concernées ont le droit de recevoir les données à caractère personnel les concernant qu'elles ont fournies à un responsable du traitement, dans un format structuré, couramment utilisé et lisible par machine, et ont le droit de transmettre ces données à un autre responsable du traitement sans que le responsable du traitement auquel les données à caractère personnel ont été communiquées y fasse obstacle […]. ».

[598] Eynard Jessica, « RGPD "empouvoirement" individuel : promesse tenue ou espoir déçu ? », Revue des affaires européennes (RAE), n° 2021/1, p. 17 : « Ce droit ne semble à ce jour pas encore mature. ».

[599] Netter Emmanuel, « La portabilité, un droit à inventer », Dalloz IP/IT, 2020, p. 352.

[600] Bellesort Julie, « Le droit à la portabilité des données à caractère personnel », *in* Bensamoun Alexandra et Bertrand Brunessen (dir.), *Le règlement général sur la protection des données, aspects institutionnels et matériels*, éd. Mare & Martin, 2020, p. 187.

[601] Paulin Boris, « La restitution des données : difficultés pratiques », Dalloz IP/IT, 2017, p. 33.

Toutefois, pour la Commission européenne, lutter contre l'exploitation abusive des données n'était pas le seul objectif du marché unique numérique. Les géants du numérique disposent d'une masse de données considérable et ne sont pas forcément enclins à les partager. Dès 2018, la Commission européenne va combattre la concentration excessive des données à caractère non personnel par certains acteurs du numérique.

II. L'ouverture des données à caractère non personnel face à la concentration abusive

212. Valeur des données à caractère non personnel. L'essor de l'Internet des objets représente une source importante de données à caractère non personnel. Parmi ces données à caractère non personnel, les informations publiques constituent une source considérable de données contribuant à améliorer le marché intérieur : les données publiques ont une valeur économique considérable[602]. Afin de promouvoir l'innovation et l'intelligence artificielle dans tous les secteurs de l'économie, une politique d'ouverture des données à caractère non personnel va être mise en place (A). Néanmoins, cette politique va faire l'objet d'un essoufflement prématuré (B).

A) Les prémisses de la politique d'ouverture des données à caractère non personnel

213. Amélioration de la circulation et de la réutilisation des données à caractère non personnel. Au regard de la valeur stratégique et économique des données publiques, une véritable politique d'*open data* a été consacrée (1). En parallèle, le Règlement (UE) 2018/1807 établissant un cadre applicable au libre flux des données à caractère non personnel dans l'Union européenne a pour dessein l'amélioration de la circulation et de la réutilisation de ces données (2).

[602] Cytermann Laurent, « L'ouverture des donnes publiques en Europe : principes et nouvelles frontières », *in* Bertrand Brunessen (dir.), *La politique européenne du numérique,* éd. Bruylant, 2023, p. 378 : « L'ouverture des données publiques constitue le prolongement à l'ère numérique du droit d'accès aux documents administratifs, garanti par le droit primaire de l'Union européenne et participe ainsi d'un idéal de transparence de l'action publique. Il est attendu d'elle qu'elle stimule le développement économique grâce à la libre réutilisation des données, dans des proportions cependant difficiles à évaluer, puisqu'elles sont comprises, selon les estimations, entre 27 milliards et 674 milliards d'euros par an à l'échelle de l'Union. ».

1. Le développement de la politique d'*open data* pour les données publiques

214. Un « domaine commun informationnel ». Dès 2015, l'avant-projet de la Loi pour une République numérique avait relevé l'idée d'un « domaine commun informationnel », contenant « les informations issues des documents administratifs diffusés publiquement », sous certaines conditions[603]. Les informations publiques seraient devenues des choses communes, au sens de l'article 714 du code civil, au même titre que l'air et l'eau[604]. Ce statut pour les données publiques n'a cependant pas été retenu pour plusieurs raisons, dont le fait que la notion d'information était trop imprécise[605]. De plus, toutes les données publiques ne sont pas diffusables et certaines font l'objet d'une redevance. Les administrations peuvent établir une redevance de réutilisation lorsqu'elles sont tenues de couvrir par des recettes propres une part substantielle des coûts liés à l'accomplissement de leurs missions de service public[606].

Les données publiques pourraient également être considérées comme des « biens publics » de nature immatérielle. Le bien public étant un bien non-rival, c'est-à-dire un bien pouvant être consommé par plusieurs personnes simultanément sans diminuer la quantité disponible pour les autres individus et un bien ne pouvant pas être individualisé. Au regard des caractéristiques des biens publics et des données, la notion de bien public paraissait appropriée. Pourtant, la circulation des données publiques rendrait la propriété de ces données incertaine[607].

215. Une « infrastructure essentielle » ou un « bien commun ». Pour d'aucuns, la donnée publique serait une infrastructure essentielle permettant une meilleure utilisation des ressources disponibles[608]. En effet, les données publiques représentent un intérêt majeur en raison du faible coût marginal de production et des fortes externalités positives qu'elles génèrent[609]. Dans un

---

603 Projet de loi pour une République numérique, Assemblée nationale, n° 3318.

604 Code civil, article 714 : « Il est des choses qui n'appartiennent à personne et dont l'usage est commun à tous. » ; Chloé Dornbierer, « Les choses non rivales : essai sur le régime juridique de l'information », Thèse, Aix-en-Provence, 2022.

605 Le projet de Loi pour une République numérique, sur lequel les citoyens ont été appelés à se prononcer, prévoyait dans son article 8 une définition positive du domaine public, intitulé « domaine commun informationnel ». Le Conseil Supérieur de la Propriété Littéraire et Artistique (« CSPLA ») a émis un avis négatif sur sa rédaction, le 3 novembre dernier, faisant suite à son « Rapport de la mission sur les enjeux de la définition et de la protection d'un domaine commun informationnel au regard de la propriété littéraire et artistique ».

606 Code des relations entre le public et l'administration, article L324-1.

607 Chevallier Jacques et Cluzel-Metayer Lucie, « L'inflexion de la notion de donnée publique », RFAP, 2018.

608 *Ibid*.

609 Boul Maxime, « Réflexions sur la notion de donnée publique », *op. cit*.

rapport intitulé « La donnée comme infrastructure essentielle », Henri Verdier met en avant un écosystème de la donnée alliant l'administration et les acteurs économiques. Au sein de cet environnement, l'État doit constituer une infrastructure de données afin d'apporter une réponse aux défis et opportunités de certains acteurs du numérique[610]. L'infrastructure permettrait une meilleure exploitation des données pour l'administration et l'ensemble des acteurs qui utilisent des données publiques. En outre, les données d'intérêt général pourraient être qualifiées de « biens communs[611] » : l'*open data* suppose de considérer les données publiques comme des biens communs pouvant échapper au régime propriétaire puisque les données doivent être libérées pour être réutilisées.

216. Évolution du cadre juridique. À l'instar des données à caractère personnel, le statut des données publiques soulève des questions complexes que le droit positif n'élucide toujours pas[612]. Les diverses notions de données publiques complexifient leur régime juridique. Actuellement, le régime des données publiques fait l'objet d'une réglementation éparse et clairsemée : la construction est évolutive et toujours en cours de construction. En pratique, la politique d'ouverture des données a guidé l'élaboration de diverses règles juridiques[613]. Tout d'abord, la Loi n° 78-753 du 17 juillet 1978 de la Commission d'accès aux documents administratifs a consacré le principe d'accessibilité aux documents administratifs par les administrés, loi fondée sur un objectif de transparence de l'administration[614]. Il s'agissait de mettre fin à ce que Jean Laveissière a pu nommer « le règne du secret[615] ». Néanmoins, selon cette conception, l'accès aux documents administratifs nécessitait une démarche proactive de l'administré auprès du service concerné. La naissance du cadre juridique de l'*open data* est apparue avec l'ordonnance n° 2005-650 du 6 juin 2005, transposant la Directive 2003/98/CE

610 Verdier Henri, « La donnée comme infrastructure essentielle », Rapport au premier ministre sur la donnée dans les administrations, 2016-2017, p. 42.

611 Danis-Fatome Anne, « Open data - Quels garde-fous pour le partage des données ? », CCE, n° 5, mai 2022.

612 Camus Aurélien, « La propriété des données publiques », *op. cit*., pp. 479-490.

613 Terrier Emilie, « Les données publiques », *in* Bruguière Jean-Michel, *L'émergence d'un droit des données*, éd. Dalloz, 2023, p. 158, précisant qu'il s'agit d'une politique avant d'être un régime juridique au regard de la définition donnée par le Journal officiel : « politique par laquelle un organisme met à disposition de tous des données numériques, dans un objectif de transparence ou fin de permettre leur réutilisation, notamment à des fins économiques », JORF, n° 0103, 3 mai 2014.

614 Loi n° 78-753 du 17 juillet 1978, codifiée au livre III du code des relations entre le public et l'administration (CRPA).

615 Laveissière Jean, « L'accès aux documents administratifs », *in* Centre Universitaire de Recherches sur l'Action Publique et le Politique (CURAPP), *Information et transparence administratives*, éd. PUF, 1988, p. 12.

du Parlement européen et du Conseil du 17 novembre 2003 concernant la réutilisation des informations du secteur public (PSI). Par-delà l'objectif d'accroître la transparence des administrations, le mouvement d'ouverture des données s'étend désormais à un objectif d'innovation économique[616]. La réutilisation des données publiques permettrait de renforcer le levier économique de l'ouverture des données. Pour développer ce levier, il convient de passer d'une logique de la détention de l'information à une logique d'ouverture et de diffusion de l'information. Dès 2011, la démarche d'ouverture est engagée par la création d'une structure administrative « Etalab » chargée de créer un portail interministériel unique des données publiques. Allant plus loin que la simple ouverture des données publiques, la Loi n° 2015-1779 du 28 décembre 2015, dite loi Valter, consacre la réutilisation gratuite des données publiques. Afin de s'adapter aux spécificités de chaque secteur, une série de législations sectorielles va être adoptée.

217. Multiplication de législations sectorielles. L'année 2015 a marqué un tournant législatif avec l'adoption de plusieurs lois sectorielles : la Loi n° 2015-990 du 6 août 2015 pour la croissance, l'activité et l'égalité des chances économiques[617], la Loi n° 2015-992 du 17 août 2015 relative à la transition énergétique pour la croissance verte, la Loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé afin de développer l'*open data* dans le secteur de la santé[618]. L'année suivante, la Loi n° 2016-1321 pour une République numérique a marqué la consécration du principe d'*open data* par défaut en France en favorisant la circulation des données à travers l'ouverture des données publiques et d'intérêt général, la création d'un service public de la donnée et le libre accès aux écrits de la recherche publique. Pour autant, certains

[616] Cytermann Laurent, « L'ouverture des donnes publiques en Europe : principes et nouvelles frontières », *in* Bertrand Brunessen (dir.), *La politique européenne du numérique,* éd. Bruylant, 2023, p. 378.

[617] Loi n° 2015-990 du 6 août 2015 pour la croissance, l'activité et l'égalité des chances économiques, article 4, modifiant l'article L1115-1 du code des transports comme suit : « Les données des services réguliers de transport public de personnes et des services de mobilité sont diffusées librement, immédiatement et gratuitement en vue d'informer les usagers et de fournir le meilleur service, notamment en permettant l'organisation optimale des services de mobilité et des modes de transport. Dans ce but, elles sont diffusées par voie électronique, au public et aux autres exploitants, dans un format ouvert destiné à permettre leur réutilisation libre, immédiate et gratuite. ».

[618] Loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé avec la création du SNDS : le système national des données de santé qui centralisera les données des bases existantes. La base va regrouper : les données les données issues des systèmes d'information des établissements de santé, les données issues des systèmes d'information de l'Assurance maladie, des informations transmises, sous forme d'échantillons représentatifs, par les mutuelles à propos des remboursements, les données sur les causes de décès et les données médicosociales issues des systèmes d'information des maisons départementales des personnes handicapées.

obstacles persistent à la diffusion et à la réutilisation complète des données publiques. Le rapport Bothorel « Pour une politique publique de la donnée » révèle que seule une minorité d'acteurs publics se conforme à la politique d'*open data*[619]. Pour l'instant, les administrations ne s'approprient pas encore les enjeux et l'intérêt de l'ouverture des données[620] .

218. Directive 2019/1024/UE du 20 juin 2019 (ISP). Pourtant, le potentiel économique de l'ouverture des données publiques est considérable. La Directive 2003/98/CE du Parlement européen et du Conseil du 17 novembre 2003 concernant la réutilisation des informations du secteur public a été révisée par la Directive (UE) 2019/1024 du Parlement européen et du Conseil du 20 juin 2019 concernant les données ouvertes et la réutilisation des informations du secteur public concernant les données ouvertes et la réutilisation des informations du secteur public[621]. La directive est entrée en vigueur le 26 juin 2019 et fut adoptée dans un climat consensuel, démontrant la volonté des états à favoriser l'innovation par l'ouverture des données publiques[622]. L'objectif était de mettre à jour le cadre juridique afin de prendre en compte les évolutions technologiques. Les modifications apportées réduisent les barrières à l'entrée sur le marché, en particulier pour les petites et moyennes entreprises en limitant la possibilité de redevances pour les administrations. Cela permet également d'accroître la disponibilité des données en intégrant dans le champ d'application de nouveaux types de données publiques et financées par des fonds publics. Enfin, cela relance les opportunités commerciales en encourageant la diffusion de données dynamiques via des interfaces de programmation d'applications (API)[623].

---

619 Bothorel Eric, « Pour une politique publique de la donnée », Rapport, décembre 2020, p. 70 : « Au-delà de cet indice, ce sont surtout les auditions de la mission et les informations collectées auprès des administrations centrales qui révèlent un manque profond d'appropriation de la politique de la donnée. Plusieurs administrations ont ainsi considéré ne pas être concernées par les sollicitations de la mission, et ont tardé à apporter une réponse malgré les relances de la mission. Une direction générale a par exemple répondu qu'elle ne produisait pas de donnée car elle n'était pas un service statistique ministériel. Ces réactions sont révélatrices de la place que beaucoup de directions métiers réservent à la donnée dans le pilotage de leurs politiques. ».

620 Cytermann Laurent, « L'ouverture des donnes publiques en Europe : principes et nouvelles frontières », *in* Bertrand Brunessen (dir.), *La politique européenne du numérique*, éd. Bruylant, 2023, p. 383.

621 La valeur économique directe totale des ISP devrait passer d'une valeur de référence de 52 milliards d'euros en 2018 pour les pays de l'UE et le Royaume-Uni à 194 milliards d'euros en 2030.

622 Castets-Renard Céline, *Droit du marché unique numérique et intelligence artificielle,* éd. Bruylant, 2020, p. 304.

623 Directive 2019/1024/UE du 20 juin 2019 concernant les données ouvertes et la réutilisation des informations du secteur public, article 3 paragraphe 1.

En parallèle de la politique d'*open data*, la promotion de l'économie des données à caractère non personnel va être consacrée par un principe de libre circulation des données à caractère non personnel.

2. L'instauration du principe de libre circulation pour les données à caractère non personnel

219. Une économie fondée sur les données. Dès 2017, dans le cadre de sa stratégie pour un marché unique numérique, la Commission européenne avait proposé des solutions juridiques visant à libérer le potentiel de l'économie fondée sur les données dans l'Union Européenne[624]. Le développement de l'Internet des objets, l'intelligence artificielle et l'apprentissage automatique représentent des sources importantes de données à caractère non personnel[625]. La libre circulation de ces données permet de rendre disponible une grande quantité de données favorisant l'essor de l'intelligence artificielle[626]. Typiquement, le développement de l'intelligence artificielle dépend de la libre circulation des données à caractère non personnel afin de produire des externalités positives[627]. De surcroît, la disponibilité des données va également favoriser la création de nouveaux services et le renforcement de la compétitivité des entreprises européennes. Pour ce faire, il était nécessaire de créer un environnement juridique adapté à la libre circulation des données à caractère non personnel. Les restrictions injustifiées à la libre circulation étaient *a priori* susceptibles d'entraver le développement de l'économie sur les données[628].

---

624 Commission européenne, « Créer une économie européenne fondée sur les données », Communication de la commission au parlement européen, au conseil, au comité économique et social européen et au comité des régions, COM(2017) 9 final.

625 Règlement (UE) 2018/1807 du Parlement européen et du Conseil du 14 novembre 2018 établissant un cadre applicable au libre flux des données à caractère non personnel dans l'Union européenne, considérant 9.

626 Castets-Renard Céline, *op. cit*., p. 219.

627 Favro Karine, « "Les données non personnelles" : un nouvel objet juridique », Dalloz IP/IT, n° 4, 2020, p. 234.

628 Commission européenne, *op. cit.*, p. 2 : « On estimait que l'économie fondée sur les données représentait 257 milliards d'euros dans l'UE en 2014, soit 1,85 % du PIB de l'Union. En 2015, ce chiffre est passé à 272 milliards d'euros, soit 1,87 % du PIB de l'Union (croissance de 5,6 % en glissement annuel). Selon la même estimation, si les conditions-cadres politiques et juridiques relatives à l'économie fondée sur les données sont mises en place en temps voulu, cette économie devrait représenter 643 milliards d'euros d'ici à 2020, soit 3,17 % du PIB global de l'Union. ».

220. Règlement (UE) 2018/1807 du Parlement européen et du Conseil du 14 novembre 2018. Le règlement établissant un cadre applicable au libre flux des données à caractère non personnel dans l'Union européenne est applicable depuis le 28 mai 2019. Ce dernier identifie deux types d'obstacles à la libre circulation de ces données : les réglementations nationales en matière de localisation des données et les pratiques menant à une dépendance à l'égard des fournisseurs dans le secteur privé. Tel que son intitulé l'indique, le règlement vise à assurer le libre flux des données à caractère non personnel au sein de l'Union[629]. Il ne s'applique pas aux opérations de traitement ayant lieu en dehors de l'Union européenne ni aux exigences de localisation relatives à ces données[630]. Ainsi, conformément à l'article 2 paragraphe 1 du règlement, le champ d'application est limité aux traitements de données à caractère non personnel dans l'Union fournis en tant que service aux utilisateurs résidant ou disposant d'un établissement dans l'Union, par un fournisseur de services établi ou non dans l'Union ou effectués par une personne physique ou morale résidant ou disposant d'un établissement dans l'Union pour ses propres besoins. La notion de données à caractère non personnel étant entendue largement puisqu'il s'agit de l'ensemble des données numériques qui n'entrent pas dans le champ des données à caractère personnel. Le champ d'application n'est nullement restreint aux données du secteur public mais couvre l'ensemble des données à caractère non personnel : il peut s'agir de données sur l'agriculture de précision[631], de données sur les besoins d'entretien des machines industrielles ou encore l'ensemble les données anonymisées[632].

221. Suppression des exigences de localisation des données. Afin de libérer le flux des données à caractère non personnel, le règlement supprime toute forme de restriction géographique. L'article 4 du règlement interdit les exigences de localisation des données contenues : tant dans les mesures directes que les mesures indirectes[633]. Par exemple, pour les mesures directes, il peut s'agir d'une obligation de stocker les données dans un emplacement géographique précis ou une obligation de respecter des exigences propres à un État membre.

---

629 Règlement (UE) 2018/1807 du Parlement européen et du Conseil du 14 novembre 2018 établissant un cadre applicable au libre flux des données à caractère non personnel dans l'Union européenne, article 1 : « Le présent règlement vise à assurer le libre flux de données autres que les données à caractère personnel au sein de l'Union, en établissant des règles concernant les exigences de localisation des données, la disponibilité des données pour les autorités compétentes et le portage des données pour les utilisateurs professionnels. ».

630 *Ibid.*, considérant 15.

631 Ces données peuvent par exemple aider à contrôler et à optimiser l'utilisation des pesticides et de l'eau.

632 Règlement (UE) 2018/1807 du Parlement européen et du Conseil du 14 novembre 2018 établissant un cadre applicable au libre flux des données à caractère non personnel dans l'Union européenne, considérant 9.

633 *Ibid.*, article 3, paragraphe 5.

Quant aux exigences indirectes de localisation de données, il peut s'agir par exemple d'une exigence d'utiliser des moyens techniques certifiés ou agréés par un État membre particulier ou d'autres exigences qui ont pour conséquence de rendre plus difficile le traitement de données en dehors de l'Union Européenne[634]. À titre d'exemple, la France imposait aux collectivités territoriales d'héberger leurs données sur un « *cloud* souverain », c'est-à-dire français[635]. Depuis l'entrée en vigueur du règlement, la circulaire a été supprimée. Toutefois, le règlement précise que les opérateurs restent libres de conclure des contrats précisant la localisation des données[636].

222. L'unique exception : la sécurité publique. L'unique exception inscrite dans le règlement est relative à la sécurité publique. En effet, le principe de libre circulation des données à caractère non personnel peut être restreint ou interdit lorsque cela se justifie par des motifs de sécurité publique[637]. Selon le considérant 19, la notion de sécurité publique - au sens de l'article 52 du traité sur le fonctionnement de l'Union Européenne et telle que l'interprète la Cour de Justice -, englobe à la fois la sécurité intérieure et extérieure d'un État membre, mais aussi les questions de sûreté publique, afin de faciliter la détection des infractions pénales, les enquêtes et les poursuites en la matière[638]. La sécurité publique présuppose l'existence d'une menace réelle et suffisamment grave portant atteinte à l'un des intérêts fondamentaux de la société, telle qu'une menace pour le fonctionnement des institutions et des services publics essentiels et pour la survie de la population, ainsi que le risque d'une perturbation grave des relations extérieures ou la coexistence pacifique des nations, ou un risque pour les intérêts militaires[639]. Ainsi, toute exigence de localisation des données qui se justifie par des motifs de sécurité publique doit être proportionnelle conformément à la jurisprudence de la Cour de justice de l'Union européenne. Les mesures doivent être appropriées pour garantir la réalisation de l'objectif poursuivi et ne doivent pas aller au-delà de ce qui est nécessaire pour atteindre cet

634 Règlement (UE) 2018/1807 du parlement européen et du conseil du 14 novembre 2018 établissant un cadre applicable au libre flux des données à caractère non personnel, considérant 4.
635 Note d'information n° 2016/004 du 5 avril 2016 relative à l'informatique en nuage (cloud computing).
636 Règlement (UE) 2018/1807 du parlement européen et du conseil du 14 novembre 2018 établissant un cadre applicable au libre flux des données à caractère non personnel, considérant 4 : « Le présent règlement ne limite en rien la liberté des entreprises de conclure des contrats précisant où les données doivent être localisées. Le présent règlement vise simplement à sauvegarder cette liberté en permettant de convenir d'une localisation située en tout lieu de l'Union. ».
637 Règlement (UE) 2018/1807 du parlement européen et du conseil du 14 novembre 2018 établissant un cadre applicable au libre flux des données à caractère non personnel, considérant 10.
638 V. par exemple l'arrêt de la CJUE du 23 novembre 2010, C-145/09, point 43.
639 V. par exemple l'arrêt de la CJUE du 22 décembre 2008, C-161/07, point 35.

objectif. *In fine*, l'unicité de cette exception démontre qu'aucune autre exception ne doit entraver le libre flux des données à caractère non personnel.

223. Améliorer la concurrence entre les services par la création d'un droit de portage. Par ailleurs, l'un des objectifs du règlement est d'encourager une concurrence effective entre opérateurs afin de permettre à un contractant de récupérer ses données auprès du fournisseur de service de *cloud* dans le but de changer de prestataire[640]. En pratique, les prestataires font en sorte de verrouiller les données dans leur système, par exemple en raison d'un format de données spécifiques ou de dispositions contractuelles, pour que l'utilisateur ne puisse pas changer de fournisseur de services. Afin d'améliorer la concurrence et les droits des utilisateurs, le règlement instaure un droit de portage pour les données à caractère non personnel. La genèse du droit de portage pour ces données est le droit à la portabilité des données à caractère personnel consacré par le Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel. Pour ce faire, le règlement instaure un cadre juridique souple[641] : les considérants du règlement sur le libre flux des données à caractère non personnel préconisent l'autorégulation des acteurs par des codes de conduite[642]. Conformément à l'article 6, un certain nombre d'aspects doivent être pris en compte lors de l'élaboration des codes de conduite sur le portage de données comme : les bonnes pratiques qui facilitent le changement de fournisseur de services et le portage des données dans des formats structurés, usuels et lisibles par machine ; les exigences minimales d'information ; les approches en matière de dispositifs de certification afin de faciliter la comparabilité des services en nuage ainsi que les feuilles de route de communication afin d'informer sur les codes de conduite. D'une manière quelque peu utopique,

---

640 Règlement (UE) 2018/1807 sur le libre flux des données à caractère non personnel, article 6.

641 Bougeard Aurélien, « Les dispositions relatives à l'accès et au portage des données : code de bonne conduite et bonnes pratiques », Dalloz IP/IT, 2020, p. 408.

642 Règlement (UE) 2018/1807 sur le libre flux des données à caractère non personnel, considérant 30 :
« Pour tirer pleinement parti de l'environnement concurrentiel, les utilisateurs professionnels devraient être en mesure de faire des choix en connaissance de cause et de comparer facilement les différentes composantes des divers services de traitement des données proposés dans le marché intérieur, notamment en ce qui concerne les conditions générales contractuelles de portage des données lors de la résiliation d'un contrat. Afin de s'aligner sur le potentiel d'innovation du marché et de tenir compte de l'expérience et de l'expertise des fournisseurs de services et des utilisateurs professionnels des services de traitement des données, les informations et exigences fonctionnelles détaillées concernant le portage des données devraient être définies par les acteurs du marché dans le cadre de l'autorégulation, encouragée, facilitée et contrôlée par la Commission, sous la forme de codes de conduite de l'Union pouvant comporter des conditions générales contractuelles types. ».

l'autorégulation permettrait aux acteurs d'adapter spécifiquement les normes à leurs pratiques. En réalité, l'autorégulation sert parfois aux géants du numérique à ne pas être contraints par des normes de « droit dur ».

Ainsi, les objectifs de libéralisation des flux de données à caractère non personnel sont louables d'un point de vue économique. En réalité, cette politique d'ouverture a fait l'objet d'un essoufflement prématuré, profitant rarement aux cibles du règlement, c'est-à-dire les entreprises européennes.

B) L'essoufflement prématuré de la politique d'ouverture des données à caractère non personnel

224. Les balbutiements d'une politique globale. Le règlement sur le libre flux des données a constitué le balbutiement d'une politique globale d'ouverture des données à caractère non personnel. Pour autant, les exigences de localisation n'étaient et ne sont pas réellement les barrières exclusives à la libre circulation des données à caractère non personnel. De surcroît, il existe des difficultés pratiques à appliquer effectivement le règlement (1). Finalement, l'étude approfondie du règlement consacre un bilan décevant (2).

1. Les difficultés pratiques d'ouverture des données à caractère non personnel

225. Le manquement de cible. En pratique, le flux des données à caractère non personnel n'est pas exclusivement limité par les exigences de localisation[643] : le nombre d'obligations nationales de localisation est faible et ne concerne qu'un petit nombre de données concernées[644]. Une étude d'impact révèle qu'il n'existe qu'une cinquantaine de textes pouvant restreindre la liberté de circulation des données à caractère non personnel. Par la suite, la Commission a abaissé ce chiffre et ne concernerait en moyenne qu'une restriction par État membre[645]. Il est

643 Zolynski Célia, « La place du règlement (UE) 2018/1807 dans la construction du droit des données de l'Union européenne », Dalloz IP/IT, 2020, p. 429.

644 Sénat, Proposition de résolution européenne portant avis motivé, n° 80 (2017-2018), déposée au Sénat le 9 novembre 2017, p. 3.

645 Mouchette Julien, « Haro sur les obligations de localisation des données non personnelles », Dalloz IP/IT, 2020, p. 401, « Lors des premières réunions du groupes Télécoms du conseil, la Commisison a abaissé ce chiffre à une quarantaine, dont un tiers serait, selon elle, justifiable au titre de la "sécurité publique" (Proposition de Résolution, n°80 (2017-2018) de S. Sutour, déposée au Sénat le 9 novembre 2017, p. 6). Au

donc contestable de fonder un règlement sur les exigences de localisation, qui ne constituent - à l'étude - qu'une problématique mineure du partage des données à caractère non personnel.

226. La rétention des données. Les restrictions de partage des données à caractère non personnel ne sont pas fondées sur les exigences de localisation, mais bien sur les pratiques des géants du numérique. L'expansion de ces acteurs du numérique repose sur la collecte et le traitement de silos des données à caractère non personnel et données à caractère personnel[646]. L'entière maîtrise des données leur permet de se développer sur de nouveaux secteurs tels que la banque, l'automobile ou encore le médical[647]. Ainsi, au-delà des frontières territoriales, les principales barrières à la libre circulation des données se situeraient au niveau des stratégies de *lock-in* et de rétention des données entre acteurs économiques. La libre circulation des données doit s'analyser « trans-plateformes » plutôt que « trans-frontières »[648].

227. Frontière incertaine des notions. En effet, ce ne sont pas les États membres qui sont réticents à partager leurs données à caractère non personnel : ce sont les géants du numérique les possesseurs de la majorité des données de la planète. Grâce à la frontière poreuse entre les notions de données à caractère personnel et de données à caractère non personnel, ils ont pu pendant longtemps récolter une masse impressionnante de données sans obligation d'ouverture. Par ailleurs, le fait d'écarter la protection aux données anonymisées permet à ces acteurs de traiter des données potentiellement à caractère personnel[649] : le risque de réidentification est

final, ce serait donc une petite trentaine de restrictions concernant donc très peu de données, qui seraient un frein à la libre circulation, soit environ - en moyenne - une par Etat membre. ».

646 Benabou Valérie-Laure, « Une cinquième liberté de circulation numérique ? Est-ce possible ? Est-ce utile ? », RTD eur., 2021, p. 286 : « Il n'est pas davantage nécessaire de s'épancher sur le fait que l'essentiel des transactions économiques est réalisé par des acteurs extra-européens (Facebook, Google, Amazon, Netflix…), dont la plupart détiennent également des éléments d'infrastructure des réseaux. Par conséquent, non seulement les circulations s'opèrent indifféremment et dans et hors le marché, pour des raisons techniques, mais encore, elles sont la plupart placées sous le contrôle d'opérateurs extra-européens. […] Dans ce contexte, la mise en place d'une liberté de circulation intra-européenne manque singulièrement de sens. ».

647 Strowel Alain, « Les données : des ressources en quête de propriété », *in* De Terwangne Cécile, Degrave Elise, Queck Robert, Dusollier Séverine (dir.), *Law, norms and freedoms in cyberspace. Droit, normes et libertés dans le cybermonde. Liber amicorum Yves Poullet*, éd. Larcier, 2018, p. 251.

648 CNnum, « La levée des obligations de localisation des données », Avis sur la libre circulation des données en Europe, 2017, Fiche, p. 4 : « Les principales barrières à la croissance d'une économie de la donnée innovante se situent moins au niveau des frontières nationales, du fait des obligations de localisation, qu'au niveau des stratégies de lock in et de rétention de données entre acteurs économiques. ».

649 Poullet Yves, « "La troisième voie", une voie difficile. Quelques réflexions autour de la politique européenne en matière d'intelligence artificielle », Revue Lamy Droit de l'Immatériel, n° 182, 1er juin 2021.

prégnant et les techniques ne cessent d'évoluer[650]. Ainsi, l'objectif d'ouverture des données à caractère non personnel est contreproductif au regard des géants du numérique : ils ne sont pas contraints à partager leurs données, en revanche, ils peuvent profiter de l'ouverture des données à caractère non personnel au niveau européen.

228. Les obstacles techniques. Par ailleurs, à l'instar des difficultés d'interopérabilité pour les données à caractère personnel, les données à caractère non personnel peuvent faire l'objet d'obstacles techniques[651]. Afin d'être utilisées de manière efficiente, les données doivent être assorties de documentation. L'utilisateur des données doit procurer une documentation au réutilisateur afin de garantir l'efficacité de la réutilisation mais la documentation nécessite un effort de la part du producteur, parfois plus lourd que celui de la production[652]. En réalité, les administrations publiques ne disposent pas des compétences nécessaires et des moyens techniques[653]. Au demeurant, lorsqu'un acteur de mauvaise foi ne documente pas ses données ou pire, modifie ses données, l'opérateur suivant ne pourra pas réutiliser les données de manière efficiente[654]. Afin d'éviter ces comportements anticoncurrentiels, le règlement sur les données à caractère non personnel recourt au droit souple. Contrairement aux données à caractère personnel, il s'agit principalement d'une prévention libre[655]. En réalité, le recours au droit souple a malencontreusement montré ses limites en présence d'acteurs malhonnêtes.

L'analyse de ces obstacles techniques et juridiques entraîne *de facto* un bilan insatisfaisant du principe des données à caractère non personnel.

---

650 Maxwell Winston, « Données publiques et données personnelles : un "mariage pour tous" aux limites de la légalité », 22 juillet 2013, édition Multimédia, n° 84.

651 Petel Antoine, « Quel bilan normatif pour l'Europe numérique ? », LexisNexis, Europe, n°5, mai 2024, p. 4 : « Le premier [reproche] est que ces textes risquent de complexifier l'essor des nouvelles technologies en Europe à travers les lourdeurs administratives et les coûts de mise en conformité qu'ils engendrent. Ce problème est particulièrement prégnant pour les petites et moyennes entreprises, les administrations ou les professions libérales qui ne disposent pas nécessairement des ressources adéquates pour y faire face. ».

652 Mouchette Julien, *op. cit*.

653 Mouncif-Moungache Mouna, « Le règlement sur la gouvernance des données ou l'émergence d'un modèle européen », *in* Eynard Jessica et Castets-Renard Céline (dir.), *Un droit de l'intelligence artificielle. Entre règles sectorielles et régime général. Perspectives comparées*, éd. Bruylant, 2023, p. 507 : « Il apparaît donc que l'ouverture des données nécessite des compétences et des infrastructures matérielles qui ne sont pas nécessairement à la portée de toutes les entités publiques, telles que les collectivités locales par exemple. ».

654 Eréséo Nicolas, « Libre circulation des données et droit de la concurrence (à propos du règlement du 14 novembre 2018 relatif à la libre circulation des données non personnelles) », Dalloz IP/IT, 2020, p. 414.

655 Bougeard Aurélien, « Les dispositions relatives à l'accès et au portage des données : code de bonne conduite et bonnes pratiques », Dalloz IP/IT, 2020, p. 408.

2. Le bilan insatisfaisant du principe d'ouverture des données à caractère non personnel

229. Bilan décevant. Le règlement sur la libre circulation des données à caractère non personnel semble avoir été adopté dans la précipitation[656]. Le règlement n'évoque pas les cibles adéquates et l'autorégulation est utopique lorsqu'elle est destinée à certains acteurs de mauvaise foi. La France se plaçait pourtant en avant-gardiste au sujet d'ouverture des données. En réalité, le rapport Bothorel du 23 décembre 2020 évoque une « avance acquise fragile »[657] et confirme le manque de qualité et d'accessibilité des données dû à une documentation trop faible et l'absence de standards interopérables. Pire encore, le rapport confirme la mauvaise foi des acteurs ayant des comportements volontaires et surtout néfastes sur la qualité des données : « certaines données peuvent aussi n'être pas exploitables en raison d'une volonté manifeste du producteur de limiter la réutilisation. Dans ces cas, la base est officiellement ouverte mais en pratique inexploitable, par exemple dans le cas d'une base de données impossible à interpréter, en l'absence d'identification des variables et de documentation suffisante[658]. ». Ainsi, la Commission européenne a complété les dispositifs d'ouverture des données à caractère non personnel par de nouveaux règlements[659].

230. Création d'un nouveau règlement sur l'ouverture des données à caractère non personnel. D'une manière regrettable, l'adoption du règlement relatif à des règles harmonisées sur un accès équitable aux données et sur leur utilisation permet de démontrer le bilan décevant du règlement sur le libre flux des données à caractère non personnel[660]. En effet, l'entrée en vigueur d'un règlement ayant le même objet est un aveu acerbe de l'échec du Règlement 2018/1807 sur le libre flux des données à caractère non personnel. Lors de l'analyse des considérants du Règlement (UE) 2023/2854 du Parlement européen et du Conseil du 13

656 Mouchette Julien, *op. cit*.
657 Mission Borthorel, « Pour une politique publique de la donnée », rapport, p. 67 : « L'essentiel des progrès réalisés par la France dans les classements internationaux est intervenu avant 2017, les places et positions n'ayant pas évolué depuis cette date (stable pour les deux classements de référence, renouvelés depuis 2017, l'OCDE et le portail européen des données). Les résultats des trois sous indicateurs utilisés par l'OCDE progressent également peu : la disponibilité de la donnée est certes passée d'une note de 0,28 à 0,30 entre 2017 et 2019, mais l'accessibilité reste notée à 0,31, sans progrès depuis 2017. ».
658 *Ibid.*, p. 70.
659 Pour l'analyse des nouveaux règlements, v. chapitre 2.
660 Proposition de règlement relatif à des règles harmonisées sur un accès équitable aux données et sur leur utilisation (règlement sur les données), COM(2022) 68 final.

décembre 2023 concernant des règles harmonisées portant sur l'équité de l'accès aux données et de l'utilisation des données (règlement sur les données) le règlement évoque effectivement une « l'efficacité limitée des cadres d'autorégulation[661] ».

[661] *Ibid*., considérant 79 : « Compte tenu de l'adoption limitée des cadres d'autorégulation mis au point à cette fin et de l'indisponibilité générale de normes et d'interfaces ouvertes, il est nécessaire d'adopter un ensemble d'obligations réglementaires minimales pour les fournisseurs de services de traitement de données afin d'éliminer les obstacles précommerciaux, commerciaux, techniques, contractuels et organisationnels, lesquels ne se limitent pas à la réduction de la vitesse de transfert des données lors du désengagement du client, qui freinent le changement effectif de services de traitement de données. ».

231. Conclusion de la section. La prise en compte d'objectifs antinomiques - la protection des données à caractère personnel et l'ouverture des données à caractère non personnel - a entraîné la construction d'un cadre normatif à la cohérence fragile. En effet, chaque type de données engendre un régime juridique différent, que ce soient les données à caractère personnel, les données à caractère non personnel ou encore les données publiques. Les données font l'objet d'un régime juridique antagoniste selon leur nature. Par ailleurs, certaines données peuvent être soumises à des sous-régimes, à l'instar des données de santé ou des données pénales.

Les données à caractère personnel font l'objet d'une protection contre l'exploitation abusive des acteurs du numérique et les données à caractère non personnel font l'objet d'une ouverture afin de lutter contre la concentration abusive par certains acteurs. Néanmoins, les résultats s'avèrent décevants pour la politique d'ouverture des données à caractère personnel menée jusque-là. L'ouverture des données nécessite des compétences techniques telles que l'anonymisation des données à caractère personnel ou encore l'utilisation de formats lisibles pour tous les acteurs. En pratique, les administrations ne disposent pas de la formation et des moyens techniques pour pratiquer l'anonymisation des données. En somme, il paraît difficile, voire utopique, d'établir un équilibre entre ces objectifs.

In fine, les acteurs qui profitent de l'ouverture de nos données européennes sont les géants du numérique. Actuellement, la politique d'ouverture des données à caractère non personnel ne profite pas aux acteurs européens. Pour les GAFAM, l'ouverture des données à caractère non personnel leur permet d'exploiter toujours plus de données en disposant des moyens techniques d'analyses, au contraire des administrations. L'absence de régime pour les données anonymisées leur permet de traiter des données potentiellement à caractère personnel.

En réalité, la complexité du cadre n'est pas le fruit du hasard : les géants du numérique n'hésitent pas à intégrer leurs propres intérêts en participant à la construction du cadre normatif afin de faire perdurer leurs pratiques d'exploitation des données.

Section 2 : Les conséquences de la recherche d'un équilibre utopique

232. Diversité des sources. Afin de concilier les objectifs antagonistes, la Commission européenne a multiplié les initiatives législatives. Le législateur européen souhaite réglementer et encadrer les données. Pour cela, les textes se succèdent à un rythme soutenu ces dernières années (I). En parallèle, ou plus spécifiquement en amont, les acteurs du numérique mettent en œuvre leur influence afin d'écarter ou de restreindre un maximum leurs obligations (II).

I. La multiplication excessive des normes

233. Annonce de plan. Depuis plusieurs années, les initiatives normatives ayant pour objet les données sont considérablement nombreuses (A). La profusion normative entraîne une dispersion des normes, entachant la cohérence promue du cadre normatif (B).

A) La profusion des normes

234. Flux normatif. L'essor des flux de données a nécessité un encadrement législatif adapté et novateur. Tout d'abord, la transversalité du droit des données entraîne une inévitable profusion des normes (1). Néanmoins, les flux normatifs peuvent impacter la compréhension du cadre normatif (2).

1. La transversalité du droit des données

235. Transversalité du droit du numérique. Le droit des données est un droit transversal : tous les domaines du droit en sont imprégnés et l'européanisation de ce droit participe également à cette transversalité[662]. Depuis l'entrée en vigueur du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données les normes se succèdent à un rythme immodéré. En effet, le règlement est entré en vigueur avec la Directive 2016/681 portant sur la coopération judiciaire et policière en matière

[662] Douville Thibault, *Droit des données à caractère personnel*, éd. LGDJ, 1ère édition, 2023, p. 46.

pénale formant le « Paquet européen de la protection des données à caractère personnel »[663]. Il faut ajouter à ce paquet les règles spéciales en matière de communication électronique avec la 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, dite directive « vie privée et communications électroniques »[664]. La directive a été modifiée en 2009 et est à nouveau en cours de modification[665]. Pour les données à caractère non personnel, le règlement sur le libre flux des données à caractère non personnel est entré en vigueur en 2018[666].

De manière non exhaustive, il est également possible d'évoquer le droit de la consommation. Afin de prendre en compte les données comme « un nouveau bien de consommation », les directives 2019/771 et 2019/770 sont entrées en vigueur le 11 juin 2019[667]. Il est également possible de citer la Directive 2019/1024 sur les données ouvertes et la réutilisation des informations du secteur public[668]. Par ailleurs, en matière de réglementation du numérique, plusieurs règlements sont entrés en vigueur ces dernières années : le Digital Service Act

663 Directive (UE) 2016/681 du Parlement européen et du Conseil du 27 avril 2016 relative à l'utilisation des données des dossiers passagers (PNR) pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière.

664 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).

665 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 services de communications électroniques, 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).

666 Règlement (UE) 2018/1807 du Parlement européen et du Conseil du 14 novembre 2018 établissant un cadre applicable au libre flux des données à caractère non personnel dans l'Union européenne.

667 Directive (UE) n° 2019/770 relative à certains aspects concernant les contrats de fourniture de contenus numériques et de services numériques et de la directive (UE) n° 2019/771 relative à certains aspects concernant les contrats de vente de biens ; Ho-Dac Marion, « Les données numériques comme biens de consommation - Approche de droit européen des contrats », *in* Nevejans Nathalie (dir.), *Données et technologies numériques*, éd. Mare et Martin, 2021, p. 49.

668 Directive (UE) 2019/1024 du Parlement européen et du Conseil du 20 juin 2019 concernant les données ouvertes et la réutilisation des informations du secteur public.

(DSA)[669], le Digital Market Act (DMA)[670], le Data Act (DA)[671], le Data Governance Act (DGA)[672] ou encore l'Intelligence Artificial Act (IA)[673]. Récemment, la Commission européenne a présenté son projet de règlement sur le futur espace européen des données de santé[674].

236. Pacte vert. De manière louable, l'environnement est pris en compte depuis plusieurs années avec le « Pacte vert[675] ». L'ambition de ce dernier est de parvenir à la neutralité climatique à l'horizon 2050 tout en maintenant la compétitivité de l'industrie européenne. L'approche est à nouveau nécessairement transversale afin d'impliquer tous les domaines dans cet objectif climatique. Une fois de plus, la prise en compte d'intérêts antagonistes s'opère entre la recherche de compétitivité et le respect du climat. L'objectif nous paraît honorable, il semble cependant antinomique de développer des technologies comme l'intelligence artificielle en prenant en compte le respect l'environnement[676]. Le 24 septembre 2024, le CESE a confirmé l'impact de l'intelligence artificielle sur l'environnement : le rapport soulève que la consommation d'électricité, de métaux rares, d'eau et d'espaces artificialisés imputable à l'intelligence artificielle est en nette croissance, et « aggrave donc l'empreinte environnementale du numérique, à la fois dans ses trois briques matérielles (les terminaux, les

669 Règlement (UE) 2022/2065 du 19 octobre 2022 du Parlement européen et du Conseil relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (règlement sur les services numériques).

670 Règlement (UE) 2022/1925 du Parlement européen et du Conseil du 14 septembre 2022 relatif aux marchés contestables et équitables dans le secteur numérique.

671 Règlement (UE) 2023/2854 du Parlement européen et du Conseil du 13 décembre 2023 concernant des règles harmonisées portant sur l'équité de l'accès aux données et de l'utilisation des données (règlement sur les données).

672 Règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données (règlement sur la gouvernance des données).

673 Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle (règlement sur l'intelligence artificielle).

674 Proposition de règlement du Parlement européen et du Conseil relatif à l'espace européen des données de santé, COM(2022) 197 final.

675 Commission européenne, « Le pacte vert pour l'Europe », COM(2019) 640 final, 11 décembre 2019.

676 Hervé-Fournereau Nathalie, « Les interférences entre la politique de l'environnement et la stratégie numérique européenne - Pacte vert et boussole numérique : Balises juridique pour une double transition soutenable », *in* Bertrand Brunessen (dir.), *La politique européenne du numérique,* éd. Bruylant, 2023, p. 593 : « La Commission encourage ainsi les États membres à adopter des feuilles de route pour assurer le déploiement accéléré de la 5G à l'horizon 2025 pour la totalité des zones urbaines et grands axes de transport terrestre. En revanche, elle ne s'interroge pas sur l'empreinte environnementale d'un tel processus, préférant mettre en exergue la plus-value de la 5G […], ce rapide aperçu de cette jurisdiversité européenne confirme le caractère fragmenté et incomplet de l'appréhension actuelle des interactions entre le numérique et l'environnement ».

réseaux, les centres de données) et dans toutes les étapes du cycle de vie (fabrication, distribution, utilisation et fin de vie) »[677]. En effet, les technologies numériques représentant entre 8 et 10% de notre consommation d'énergie et 2 à 4% des émissions de gaz à effet de serre. La Commission européenne avouant elle-même qu'il s'agit certes de « petits pourcentages », mais de « gros nombres » en réalité sur l'impact environnemental[678] : l'empreinte de la donnée sur l'environnement est en réalité catastrophique[679]. Avec le « Pacte vert », il faudra veiller à ne pas présenter « l'utilisation de la donnée comme une solution magique à la diminution de l'empreinte environnementale de l'être humain afin d'éviter de traiter réellement les causes de problèmes environnementaux qui sont l'existence d'activités polluantes en elles-mêmes[680] ».

Finalement, le droit européen du numérique est devenu « une constellation normative[681] ». Les nombreuses législations représentent des flux normatifs.

2. Les flux normatifs pour les données

237. Notion de flux normatif. Avec le développement des technologies émergentes, les flux des données ne cessent de se multiplier[682], la notion de flux évoquant l'abondance ou la profusion[683]. L'ensemble des usages des données doit pourtant être encadré afin d'établir un équilibre pour la compétitivité des entreprises. Pour ce faire, l'encadrement des flux de données entraîne des « flux normatifs[684] ». Il s'agit d'établir des régimes pour la protection ou l'ouverture

677 Comité économique social et environnemental (CESE), « Impacts de l'intelligence artificielle : risques et opportunités pour l'environnement », avis, 24 septembre 2024, p. 5 : « Par exemple, en 2023, la direction d'Alphabet, la maison-mère de Google, estimait qu'un "prompt" fait à une IA générative demandait l'équivalent de dix fois l'énergie consommée par une simple recherche sur Google. Une étude récente établit que les systèmes d'IA pourraient consommer en 2027 entre 4,2 et 6,6 milliards de mètres cubes d'eau, soit une consommation légèrement supérieure à celle du Danemark et équivalente à la moitié de celle du Royaume-Uni ».

678 Commission européenne, « Secteur numérique vert. Bâtir l'avenir numérique de l'Europe », publié le 24 avril 2024, disponible sur https://digital-strategy.ec.europa.eu/fr/policies/green-digital.

679 Bessot David, Billard Pierre, Bourgeois Matthieu *et al.*, « L'empreinte de la donnée sur le vivant : Essai pour un numérique responsable », étude, 2024.

680 *Ibid.*, p. 71.

681 Bertrand Brunessen, *La politique européenne du numérique*, éd. Bruylant, 2023, p. 30.

682 Sur la notion de flux de données, v. Bougeard Aurélien, « Le phénomène de Big Data et le Droit, Pour une appréhension juridique par sa décomposition technique », Thèse, Strasbourg, 2022.

683 Définition Larousse, v° « Flux ».

684 Nicolas Émeric, *Penser les flux normatifs*, éd. Mare et Martin, 2018, p. 87 : « Les normes étant désormais produites de façon continue, le flux évoque l'idée de grande abondance, de flot de paroles ou de textes. On

des données, qu'elles soient personnelles, non personnelles, publiques ou encore industrielles. En réalité, l'expression de « flux normatif » revêt une connotation péjorative à laquelle nous souscrivons par l'intensification des normes sur une période restreinte[685] : « l'omniprésence de la loi n'est jamais le signe d'un progrès[686] ».

238. Densification normative. L'intensification normative n'est pas un phénomène récent mais l'essor des technologies et la célérité des changements ont entraîné une forte « densification normative »[687] . Afin d'accentuer le phénomène d'intensification, il est même possible de reprendre l'image d'un droit devenu « obèse[688]». La densification normative est un phénomène de société[689] : les technologies émergentes et plus particulièrement les données nécessitent des modifications itératives du droit positif. Le numérique est une matière « à rotation rapide[690] » pour lequel certaines réformes étaient indispensables : le droit doit s'adapter à ces nouvelles pratiques afin de faire face aux risques pour les individus. En réalité, la densification normative ne profite pas forcément aux individus, rendant le droit des données ésotérique et difficile à mettre en œuvre. Les géants du numérique profitent de cette multiplicité afin de rendre le cadre normatif complexe.

ne sera donc guère étonné que le mot "flux" apparaisse le plus souvent dans des propos relatifs au phénomène d'inflation normative, phénomène dont on sait l'importance depuis une trentaine d'années. ».

685 Le Goff Joan et Onnée Stéphane, *Puissances de la norme. Défis juridiques et managériaux des systèmes normatifs contemporains*, éd. EMS Éditions, 2017, p. 171.

686 Terré Francois et Molfessis Nicolas, *Introduction générale au droit*, éd. Dalloz, 2020, p. 137 : « La densification des règles affaiblit corrélativement nos libertés et dans la croyance hébétée dans les vertus d'un État-providence qui nous protégerait par le droit, il y a une évidente abdication de nos droits les plus élémentaires. ».

687 Thibierge Catherine, *Densification normative. Découverte d'un processus,* éd. Mare et Martin, 2014 ; sur la densification normative de la politique européenne numérique : Marti Gaëlle, « Les instruments normatifs de la politique numérique », *in* Bertrand Brunessen (dir.), *La politique européenne du numérique,* éd. Bruylant, 2023, p. 236 ; sur l'abondance des normes : Ollier Jean-Yves, « La gouvernance européenne des données », *op. cit*, p. 735.

688 Moreau Michel, « Sur un droit obèse », Revue de jurisprudence commerciale, n°3, p. 267.

689 Thibierge Catherine, *op. cit.*

690 Terré François et Molfessis Nicolas, *Introduction générale au droit*, éd. Dalloz, 2022, p. 420.

B) La dispersion des normes

239. Impact sur la cohérence du cadre normatif. La profusion des normes entraîne *de facto* des conséquences néfastes pour la compréhension et la cohérence du cadre normatif. Tout d'abord, il existe un risque de multiplication des sources (1) et logiquement, une altération de la cohérence du cadre normatif (2).

1. Le pluralisme normatif

240. Théorie du droit. Le célèbre juriste Hans Kelsen avait développé une théorie « pure » du droit, autrement dit, un droit épuré de toute considération politique, sociologique ou idéologique[691]. En réalité, la théorie pure du droit est mise à mal par les faits et plus particulièrement, par l'essor du numérique[692]. La difficulté du numérique réside dans la prise en compte d'intérêts et d'objectifs antagonistes[693]. Lorsqu'on observe le droit du numérique, le droit est inexorablement issu des faits, de l'économie ou encore de la sociologie. Ainsi, la complexification du monde, l'accélération du progrès technique, la dispersion des producteurs du contenu des normes sont autant d'éléments à prendre en compte afin d'analyser l'inflation normative[694]. L'inflation législative et réglementaire décrédibilise l'image de l'arbre juridique, c'est-à-dire l'image d'un système juridique ordonné et vertical. L'essor du numérique conduit à « délaisser l'image du droit sous forme d'arborescence pour lui préférer l'image du rhizome, qui configure un univers non hiérarchique, dominé par la circularité et la complexité[695] ». La complexité est complétée par l'essor des sources infra-législatives ou des « petites sources »[696].

---

691 Kelsen Hans, *Théorie pure du droit*, éd. LGDJ, 1999.

692 Jestaz Philippe, « L'erreur "fondamentale" de Kelsen », RTD civ, 2023, 832.

693 Martial-Braz Nathalie, « La transdisciplinarité du droit numérique », *Penser le droit de la pensée : Mélanges en l'honneur de Michel Vivant*, éd. Dalloz, p. 28 : « Assurer la protection de la vie privée tout en autorisant largement l'open data et l'usage des données ; préserver la liberté d'information et d'expression tout en veillant à lutter contre la diffusion de fausses informations ; protéger la liberté du commerce et de l'industrie mais réguler les plateformes pour protéger leurs utilisateurs ; favoriser l'open source tout en préservant les droits de propriété de chacun ; faciliter l'accès aux œuvres et aux créations en ligne tout en préservant le droit des auteurs, etc. ».

694 Conseil d'État, « Mesurer l'inflation normative », étude présentée le 3 mai 2018.

695 Terré François et Molfessis Nicolas, *Introduction générale au droit,* éd. Dalloz, 2020, p. 203.

696 Hachez Isabelle, Cartuyvels Yves et Dumont Hugues, *Les sources du droit revisitées. Théorie des sources du droit*, volume 4, Presses universitaires Saint-Louis Bruxelles, 2012 ; Ost Francois, Van de Kerchove Michel, De la pyramide au réseau ? Vers un nouveau mode de production du droit ?, Revue interdisciplinaires d'études juridiques, 2000.

241. Essor des sources infra-législatives. Sous la pression de la célérité du développement des technologies, le législateur partage sa souveraineté avec des sources infra-législatives[697]. Le développement du droit souple illustrerait une incapacité croissante du pouvoir politique de mettre en œuvre une régulation[698]. Néanmoins, les « petites sources » servent simplement à suppléer l'État, sans être pour autant contraignantes[699]. En droit international, il peut paraître plus consensuel dans un premier temps de recourir au droit souple plutôt qu'au droit dur. Le recours au droit souple est bénéfique pour les géants du numérique, et ils en sont conscients. Au niveau européen, il va s'agir de lignes directrices, de livres blancs ou verts. Au niveau national, la plupart des autorités administratives indépendantes vont pouvoir émettre des avis ou des recommandations dans des domaines techniques. En outre, les hautes juridictions vont pouvoir émettre des communiqués ou des rapports. L'ensemble de ces sources sont non contraignantes et ont pour fonction d'accompagner le droit dur afin de faciliter sa mise en œuvre. En pratique, le pluralisme juridique et la prise en compte d'intérêts antagonistes entachent la cohérence promue du cadre normatif.

2. L'altération de la cohérence des normes

242. L'inintelligibilité du cadre. Le domaine du numérique étant avant tout un domaine technique, il ressort une certaine inintelligibilité des textes. Il existe une pléiade de textes ayant le même objet, réduisant la cohérence du dispositif[700]. Plus le nombre de règlement augmente, plus les « petites sources » se multiplient afin de guider les protagonistes dans leur mise en conformité ; la multiplicité des sources participe *de facto* à l'inflation normative. L'inflation est l'un des facteurs prégnants de la complexité des normes s'appliquant aux données.

---

697 Magnon Xavier, « L'ontologie du droit », Revue française de droit constitutionnel, 120, Presses Universitaires de France, 2019.

698 Bernheim Emmanuelle, « Le "pluralisme normatif" », Revue interdisciplinaire d'études juridiques, 67, Université Saint-Louis, Bruxelles, 2011.

699 Larouer Marion, « Entre normes techniques et juridiques : la boîte à outils comme solution au problème de l'interopérabilité ? », *in* Eynard Jessica et Macilotti Giorgia (dir.), *L'identité numérique en construction. Quels enjeux et quels modèles ?*, éd. Bruylant, 2024, pp. 533-546.

700 Poullet Yves, « Cinq ans après - le RGPD est-il toujours la solution ? », RDTI, n° 90, 2023, p. 7 : « À un RGPD, qui compte 99 articles, là où la Convention 108+ se contente de 30 dispositions, s'ajoute la directive (UE) 2016/680, directive « Police », à la longueur et au contenu tout aussi prolifiques. […] C'est à travers ce labyrinthe de textes que le praticien de la protection des données se doit de naviguer. ».

L'augmentation des sources nuit à la cohérence et à l'accessibilité du droit[701]. Il devient utopique de connaître la loi et met donc à mal le célèbre adage selon lequel nul n'est censé ignorer la loi. Pour le Professeur Philippe Jestaz, « il faut s'y résigner : les hiérarchies qu'on prétend établir sont vaines parce que le droit naît dans le désordre et continue d'y vivre, cela d'autant qu'il cherche à coller à une réalité elle-même désordonnée[702] ». En effet, les pratiques du numérique sont mouvantes et cela rend difficile la mise en place d'un cadre normatif immuable[703].

En réalité, la fragmentation permet aux acteurs économiques de rechercher le territoire avec la norme la plus avantageuse. Le rapport d'évaluation sur le Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données a confirmé la fragmentation du dispositif : les approches divergentes et le recours au droit souple rendent le cadre particulièrement complexe[704]. En pratique, l'inintelligibilité des lois devient une opportunité pour les acteurs du numérique, inintelligibilité dont ils sont en partie les auteurs[705].

[701] Benzerafa-Alilat Manel et Gibert Patrick, « De l'inflation normative à l'amplification des lois dans le processus parlementaire », Revue française d'administration publique, 182, Institut national du service public, 2022, p. 543.

[702] Jestaz Philippe, « Droit commun et droit spécial », RTD civ., 2022.

[703] Desgens-Pasanau Guillaume, « Data Act - Nouveau règlement européen sur les données (Data Act). Quelles conséquences pour les professionnels ? Morceaux choisis et premiers éléments d'analyse », CCE, n°5, mai 2024, p. 6 : « Certes nul n'est censé ignorer la loi, force est néanmoins de constater qu'ils sont peu nombreux ceux qui parmi nous disposent à date à tout le moins d'une vision parfaitement claire des obligations qui incomberont demain aux acteurs économiques, en réconciliant et en croisant tous les textes adoptés en parallèle sur la période récente. À noter d'ailleurs que le législateur français s'obstine à vouloir adopter des textes sur des sujets désormais encadrés au niveau européen, ce qui pose la question de la pertinence et de la cohérence de certains textes franco-français au regard du droit européen, comme la loi SREN (actuellement déférée au Conseil constitutionnel). Les différentes marges de manœuvre ou renvois au droit national contribuent également à ce manque de lisibilité. ».

[704] Debet Anne et Martial-Braz Nathalie « Les sources du droit de la protection des données en question », Dalloz IP/IT, 2023, pp. 497-498.

[705] Bessot David, Billard Pierre, Bourgeois Matthieu *et al.*, « L'empreinte de la donnée sur le vivant : Essai pour un numérique responsable. », étude, 2024, p. 3 : « Les législateurs français et communautaire n'ont cessé d'adopter des textes spéciaux, que l'esprit de compromis, le défaut de vision et la puissance de certains lobbies rendaient non seulement outrageusement complexes, mais surtout d'application illusoire. » .

II. La multiplication des influences

243. Influence. La pratique du *lobbying* n'est pas une pratique nouvelle. Toutefois, la complexité et la technicité de la matière permettent une influence prégnante et collective des groupes de pression (A). Plus spécifiquement, les géants du numérique exercent une influence indécente sur l'élaboration des normes dont ils sont les protagonistes (B).

A) L'influence collective des groupes de pression

244. Relation d'interdépendance. De prime abord, la relation entre le législateur et les groupes de pression est une relation saine et d'interdépendance (1). Les groupes de pression éclairent le législateur sur certains points techniques de leur domaine de compétence afin d'élaborer conjointement des normes adéquates. Néanmoins, cette interdépendance entraîne des effets néfastes lorsque les acteurs sont de mauvaise foi (2).

1. La relation d'interdépendance entre le législateur et les groupes de pression

245. Définition des « groupes de pression ». Depuis les années 1830, le *lobbyiste* désigne celui qui fréquente les couloirs afin d'influencer les membres des assemblées législatives. Le phénomène n'est pas récent mais il s'intensifie toutefois avec les années[706]. Les groupes de pression sont définis comme des organisations exerçant une pression sur les pouvoirs publics dans le but d'obtenir des décisions conformes à leurs intérêts. L'intérêt d'un groupe de pression étant d'infléchir le sens de la norme. Selon le Professeur Lapousterle, le groupe de pression doit être distingué du *lobbying*. Le *lobbying* désigne l'activité par une structure permettant aux groupes de pression d'influencer les décisions des pouvoirs publics : il peut s'agir d'un cabinet de conseil ou d'un cabinet d'avocats par exemple[707]. Le *lobbying* devient alors un moyen d'action pour les groupes de pression afin d'imposer leurs intérêts communs. Les intérêts des groupes de pression peuvent parfois servir au législateur afin d'élaborer des normes cohérentes et effectives.

[706] Mekki Mustapha, La force et l'influence normatives des groupes d'intérêt, éd. Lextenso, 2011, p. 11-14.
[707] Jestaz Philippe, « Sources du droit, sources de droit : une cartographie », *in* Jestaz Philippe (dir.), *Mélanges en l'honneur de Philippe Jestaz. Libres propos sur les sources du droit*, éd. Dalloz, 2006.

246. Effets positifs des groupes de pression. Il existe une relation réciproque entre le législateur et les groupes de pression[708] : lorsque la matière est technique, les groupes de pression constituent une source d'information pour le législateur. Ils deviennent alors une source d'expertise nécessaire pour ce dernier afin d'élaborer des normes sur des sujets complexes[709]. Un rapport d'information sur la présence et l'influence de la France dans les institutions européennes confirme que les groupes de pression permettent aux députés européens d'avoir accès à une information diversifiée et contradictoire[710]. L'accès à cette information constitue une relation d'interdépendance entre les groupes de pression et le législateur. En ce sens, plus la matière est technique et complexe, plus le législateur sera dépendant des informations fournies par les groupes de pression[711].

247. Gage d'effectivité des normes. De surcroît, l'intervention des groupes de pression dans l'élaboration des normes est, *a priori*, un gage d'effectivité pour le législateur. En effet, l'élaboration de la loi au regard des aspirations des acteurs peut être une condition de son effectivité[712]. Le législateur permet donc aux groupes de pression d'intervenir dans l'élaboration des normes afin de faciliter leur application et d'éviter que les principaux destinataires s'y opposent[713]. En pratique, les acteurs doivent être de bonne foi pour que cette condition d'effectivité s'applique. Malencontreusement, il est possible de douter de la bonne foi des géants du numérique.

248. Encadrement des groupes de pression au niveau de l'Union. Afin de réduire les effets potentiellement néfastes des groupes de pression, le législateur européen a régulé leurs activités. Au niveau de l'Union Européenne, le *lobbying* désigne « toutes les activités menées dans le but d'influencer les politiques et les processus de décision des instruments de l'Union, quel que soit

---

[708] Mekki Mustapha, *op. cit.*, p. 33.

[709] Delmas-Marty Mireille, *La refondation des pouvoirs. Les forces imaginantes du droit (III)*, éd. Le Seuil, 2009, p. 144 : « D'abord, il faut mentionner le phénomène bien connu, notamment à Bruxelles, du lobbying, c'est-à-dire des groupes de pression censés représenter des professionnels ou des secteurs d'activité et proposant leur expertise, souvent réelle, sur des problèmes complexes. ».

[710] Rapport d'information n°1594 déposé par la délégation de l'Assemblée nationale pour l'Union européenne sur la présence et l'influence de la France dans les institutions européennes, enregistré à la présidence de l'Assemblée nationale le 12 mai 2004, p. 68.

[711] Lapousterle Jean, *L'influence des groupes de pression sur l'élaboration des normes*, éd. Dalloz, 2009, p. 21.

[712] Bergel Jean-Louis, *Théorie générale du droit*, 4ème édition, éd. Dalloz, 2003, p. 153.

[713] Lapousterle Jean, *op. cit.*, p. 32.

le lieu où elles sont réalisées et quel que soit le canal ou le mode de communication utilisé[714] ». La définition est volontairement très large et inclut six catégories principales de lobbyistes tels que les cabinets de consultants, les entreprises et associations syndicales, les groupes de réflexion et les institutions académiques, les organisations culturelles et les représentations d'autorités locales et autres entités publiques. Les activités de *lobbying* sont encadrées par un registre de transparence de l'Union Européenne : il s'agit d'une base de données dans laquelle les groupes de pressions sont répertoriés[715]. Toutes les organisations et travailleurs indépendants sont censés être répertoriés dès lors qu'ils mènent des activités dans le but d'influencer l'élaboration ou la mise en œuvre des politiques et sur les processus de décision des institutions de l'Union[716]. Pour autant, l'absence d'efficacité de cette mesure peut être relevée puisque l'inscription au registre de transparence est facultative et qu'un « bon lobbying ne se fait que dans le secret[717] ».

249. Encadrement des groupes de pression en France. En France, la Loi n° 2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique instaure un répertoire numérique national dans lequel toutes les organisations entrant régulièrement en communication avec un membre de l'exécutif ou un parlementaire afin « d'influer sur la décision publique[718] », est tenu de s'y inscrire, sous peine

---

714 Définition du lobbying par la Haute autorité de la vie publique, disponible sur https://www.hatvp.fr/lobbying/actualites/la-regulation-du-lobbying-au-niveau-de-lunion-europeenne/.

715 Selon le rapport « GAFAM Nation. La toile d'influence des géants du web en France », par l'Observatoire, publié le 13 décembre 2022, « Google a bénéficié de pas moins de 72 rendez-vous avec la Commission présidée par Ursula von der Leyen depuis son entrée en fonction en 2019. Meta en a eu 66, Microsoft 65, Apple 32 et Amazon 27. Sans oublier le principal lobby européen du secteur numérique, Digital Europe, qui en a eu 53. », disponible en ligne.

716 Rapport annuel sur le fonctionnement du registre de transparence 2016 présenté par les secrétaires généraux du Parlement européen et de la Commission, Mme Sylvie Guillaume, vice-présidente du Parlement européen et M. Frans Timmermans, premier vice-président de la Commission européenne, p. 3.

717 Bréhier Thierry, « Les groupes de pression à l'assemblée nationale », Pouvoirs, Revue française d'études constitutionnelles et politiques (n° spéc. 34), PUF, 1985, p. 107, cité par Macrez Franck, « Créations informatiques : Bouleversement des droits de propriété intellectuelle ? », Thèse, Montpellier, 2007, p. 76.

718 Loi n° 2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique, article 18-2 : « Sont des représentants d'intérêts, au sens de la présente section, les personnes morales de droit privé, les établissements publics ou groupements publics exerçant une activité industrielle et commerciale, les organismes mentionnés au chapitre Ier du titre Ier du livre VII du code de commerce et au titre II du code de l'artisanat, dont un dirigeant, un employé ou un membre a pour activité principale ou régulière d'influer sur la décision publique, notamment sur le contenu d'une loi ou d'un acte réglementaire. ».

« d'un an d'emprisonnement et de 15 000 euros d'amende[719] ». Toutefois, l'encadrement des groupes de pression en France est encore insuffisant. En effet, aucune obligation ne pèse sur les responsables publics eux-mêmes, ce sont les organisations qui doivent déclarer leurs activités. Il est légitime de se demander quels sont les intérêts pour les groupes de pression ainsi que pour les responsables politiques d'être transparents à ce sujet.

Ainsi, l'ancien vice-président de l'Assemblée nationale en charge des lobbies préconise dans un rapport de 2021 la publication des agendas des parlementaires et le *sourcing* des amendements[720]. Pour aller encore plus loin, il envisage à plus long terme de rendre obligatoire le dépôt des propositions d'amendements des *lobbies* sur une plateforme ouverte, en *open data*, sur le site de l'Assemblée. Cette mesure permettrait aux citoyens de comprendre « l'empreinte normative », c'est-à-dire l'impact réel des *lobbies* sur l'élaboration des normes[721]. La volonté de renforcement de l'encadrement des groupes de pression intervient afin d'éviter les effets négatifs, voire pervers de ces acteurs. La genèse de cet encadrement provient des polémiques lors des négociations de la loi « DADVI », illustrant une « désolante histoire de *lobbying*[722] ».

[719] Loi n° 2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique, article 18-9 : « Le fait, pour un représentant d'intérêts, de ne pas communiquer, de sa propre initiative ou à la demande de la Haute Autorité pour la transparence de la vie publique, les informations qu'il est tenu de communiquer à cette dernière en application de l'article 18-3 est puni d'un an d'emprisonnement et de 15 000 € d'amende. ».

[720] Waserman Sylvain, « Propositions pour un lobbying plus responsable et transparent », Rapport, présenté par le Vice-président de l'Assemblée nationale Président de la délégation du Bureau chargée des représentants d'intérêts et des groupes d'études, 2021.

[721] Amendement de l'Assemblée nationale du 24 septembre 2016 sur la « Transparence, lutte contre la corruption et modernisation de la vie économique », n°4045, pp. 1-2 : « L'empreinte normative consiste à joindre à un texte normatif la liste des personnes entendues par les responsables publics dans le cadre de son élaboration, de la rédaction du projet à son entrée en vigueur. Cette recherche de transparence devrait être une évidence quotidienne dans la mesure où un mandat électif est un contrat passé entre les Français et des élus, exercé sur fonds public, pour la recherche de l'intérêt général. Dans une recommandation du Conseil pour la transparence et l'intégrité des activités de lobbying, du 18 février 2010, l'OCDE indique : Les pouvoirs publics devraient également envisager de faciliter le contrôle par le public en faisant savoir qui a cherché à exercer une influence sur une loi ou une décision, par exemple en rendant publique un communiqué ou une "empreinte législative" indiquant quels sont les lobbyistes qui ont été consultés lors d'initiatives législatives. En assurant en temps utile l'accès à de telles informations, on pourra prendre en compte les différents points de vue de la société et des entreprises et disposer ainsi d'informations équilibrées pour l'élaboration et la mise en œuvre des décisions publiques. ».

[722] Dormont Sarah, « L'élaboration de la norme en droit d'auteur : les discours sur la légitimité », Légipresse, 2019, 79 ; Vivant Michel, « Les exceptions nouvelles au lendemain de la loi du 1er août 2006 », D., 2006, p. 2159, évoquant « une désolante histoire de lobbying ».

250. Encadrement inefficace. En réalité, afin d'échapper à la publication dans le registre, les avocats peuvent par exemple invoquer le secret des affaires. À ce jour, des données « douteuses » et l'absence de certains lobbies caractérisent les registres de transparence[723] . Par ailleurs, les informations à déclarer sont vagues, voire « inexistantes pour les pratiques les plus contestables »[724]. L'absence de transparence et les pratiques des groupes de pression entraînent des effets pervers.

2. Les effets pervers de la relation d'interdépendance

251. Un droit négocié. Sur les sujets techniques, la relation d'interdépendance entre le législateur et les groupes de pression peut avoir des effets pervers[725] : le législateur souhaite réguler une pratique qu'il considère comme néfaste et parallèlement, les groupes de pression souhaitent faire valoir leurs propres intérêts[726]. L'intégralité des règlements entrés en vigueur ces dernières années menace les intérêts économiques des géants du numérique. Ainsi, il est certain que les intérêts du législateur et les intérêts des groupes de pression sont antagonistes[727]. La prise en compte de ces intérêts antagonistes va inévitablement influer sur le contenu de la norme[728]. Les groupes de pression servent aux intérêts des multinationales ayant pour objectif soit d'obtenir la norme la moins contraignante soit de bloquer un projet de loi aux conséquences indésirables[729]. De surcroît, entre la volonté du législateur européen de créer un marché unique numérique avec comme principal objet l'ouverture des données et la volonté des multinationales de maintenir leur monopole sur ces dernières, les législations se succèdent par « brique », rendant la matière difficilement intelligible. De fait, la recherche d'un équilibre menée par le législateur apparaît utopique avec la présence des géants du numérique dans le processus de construction des normes.

---

[723] Selon le centre de recherche Corporate Europe Observatory.

[724] Deumier Pascale, « Reconnaissance du lobbying en France », RTD civ., 2010, p. 62.

[725] Bensamoun Alexandra, « Les mutations de la norme en droit d'auteur (réflexion sur les sources) », *in* Braz-Martial Nathalie, *Les mutations de la norme. Le renouvellement des sources du droit*, éd. Economica, 2000, p. 59.

[726] Molfessis Nicolas, « La loi de la course », RTD civ., 1998, 778 : « D'autres soulignent très subtilement que la généralisation des groupes de pression neutralise les risques de faveurs catégorielles, au profit d'un débat contradictoire mettant tous les intérêts en présence. On ne pourrait que le souhaiter. Mais la pratique est bien loin de cet idéal, qui témoigne de l'inégalité des forces en présence, d'un déséquilibre patent. ».

[727] Malinvaud Philippe, « Lobbying et construction », RDI, 2012, 361.

[728] Vallée Laurent, « Élaboration de la norme et influence », Justice et Cassation, 2012, p. 99.

[729] Barron Andrew et Voss Gregory, « La culture et son impact sur les actions politiques des entreprises », Revue française de gestion, 252, Lavoisier, 2015.

252. Un droit par étapes. Toutefois, afin de contrer ce droit par « brique », la Présidente de la Commission européenne, Ursula Von der Leyen, avait proposé à la Commission en 2019 la méthode « *one in, one out* ». Cette méthode consiste à retirer un ou plusieurs actes législatifs avant qu'un nouvel acte puisse être intégré dans l'acquis communautaire du même domaine d'action politique. Depuis une décennie, les gouvernements souhaitent freiner la croissance de la réglementation et la méthode permet d'une part, de limiter les coûts au niveau européen et d'autre part, de maintenir une certaine intelligibilité dans le domaine législatif. La méthode a été instaurée en renfort du programme pour une réglementation affûtée et performante (REFIT) de la Commission européenne. Le programme REFIT a pour objectif de simplifier la législation existante en réduisant les formalités administratives.

En réalité, le programme REFIT peut caractériser l'aveu de la commission de la surabondance et complexité des normes. Il est relevé dans le rapport « "One in, one out" dans le système juridique de l'Union Européenne, une réforme trompe l'œil ? », que l'une des raisons de l'échec de cette méthode est la « frustration du Conseil qui doit accepter des amendements dits "politiques" du Parlement européen, qui émanent souvent de groupes d'influence ou de lobbys économiques[730] ». D'autre part, il est également soulevé que « le traitement des consultations spécifiques et/ou politique est très opaque[731] ». À ce jour, l'Europe procède encore par « petits pas » ou « par brique » afin de légiférer sur les données. À titre d'illustration, le règlement e-Privacy[732] - présenté en 2017 -, est encore en négociation. Le règlement a pour principal objet les *cookies* et autres technologies de suivi. Ainsi, les acteurs du numérique exercent un *lobbying* intensif afin de retarder l'entrée en vigueur du règlement, susceptible d'entraver leurs pratiques à ce sujet.

[730] Van den Abeele Eric, « "One in, one out" dans le système juridique de l'Union Européenne, une réforme trompe l'œil ? », Working Paper, Institut syndical européen, avril 2020, p. 14.
[731] *Ibid.*
[732] Proposition de règlement du parlement européen et du conseil concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques et abrogeant la directive 2002/58/CE (règlement «vie privée et communications électroniques»), COM/2017/010 final - 2017/03.

B) L'influence spécifique des acteurs du numérique

253. Influence des géants du numérique. En effet, la puissance des GAFAM leur permet d'exercer des campagnes intenses de *lobbying* au sujet de normes dont ils sont les principaux acteurs. Les acteurs du numérique exercent une influence néfaste sur l'élaboration des normes (1), influence incontestable au regard de leurs dépenses à ce sujet (2).

1. L'influence néfaste des GAFAM

254. La puissance des multinationales. Les multinationales ont pris une place incontestable dans l'élaboration des normes[733]. L'importance de leur puissance économique et le rayonnement mondial de leurs services leur permettent d'imposer leurs propres règles[734]. Il existe désormais une co-production de la norme grâce aux procédés de *lobbying* de ces multinationales[735]. Elles prônent l'autorégulation grâce à l'élaboration de droit souple leur permettant d'échapper à certaines de leurs obligations. La logique verticale du processus normatif s'est substituée à une logique horizontale reposant sur la coopération entre les acteurs du numérique et les pouvoirs publics[736]. Néanmoins, les acteurs du numérique servent en priorité leurs intérêts économiques, mettant en péril la protection des intérêts des utilisateurs. En réalité, ils cherchent à développer une régulation privée en marge du droit étatique[737]. Les acteurs du numérique bénéficient d'arguments intéressants pour les États membres comme l'installation d'infrastructures et par voie de conséquence, la création d'emplois[738]. Les multinationales exerçant une influence sur l'élaboration des normes au sujet des données sont majoritairement les géants du numérique.

---

733 Delmas-Marty Mireille, *op. cit*., voir le chapitre I sur la prépondérance des acteurs économiques.

734 Lequette Suzanne, *op. cit*., p. 84.

735 Caire Anne-Blandine, *Les nouveaux pouvoirs*, éd. Bruylant, 2017.

736 Lequette Suzanne, *op. cit.,* p. 47.

737 Ost François et Van de Kerchove Michel, « De la pyramide au réseau ? », Revue interdisciplinaire d'études juridiques, Volume 44, Université Saint-Louis, Bruxelles, 2000, p. 65 : « Mille formes de pouvoirs privés dont certains disposent de budgets considérables (parfois supérieurs à ceux de certains États) ainsi que d'une capacité d'action politique non négligeable (on songe aux grandes entreprises sur le terrain économique et social). ».

738 Selon le journaliste Andreas Vou : « les centres de données ont généré 7,13 milliards d'euros en Irlande depuis 2010. L'organisation Host in Ireland estime que les investissements dans les centres de données engendreront un profit de 1,13 milliard d'euros en 2020, avec 12 infrastructures en cours de construction et 26 supplémentaires prévues. Elle prévoit 6,7 milliards d'euros d'investissements d'ici à 2025, ajoutant aux 6,2 milliards déjà investis dans le secteur […] Une telle évolution de la société est une aubaine pour les géants de la technologie, qui pourront sans difficulté imposer et faire prévaloir les lois qui servent leurs intérêts, car ils seront au cœur de l'économie des nations et des infrastructures. ».

255. Les GAFAM : la plus grande industrie de *lobbying*. Le modèle d'affaire de ces multinationales repose sur les données. Ainsi, lorsque l'Union européenne dévoile sa stratégie législative pour encadrer l'utilisation des données, les géants du numérique investissent dans le *lobbying*. L'intérêt de ces acteurs est d'influencer les normes sur ce sujet afin d'obtenir la réglementation la moins stricte pour préserver leur modèle commercial et d'augmenter leurs bénéfices[739] : en réalité, l'aspiration de ces acteurs est de préserver leurs intérêts financiers au détriment des droits fondamentaux des citoyens. Pour ce faire, les GAFAM bénéficient d'un accès disproportionné aux décideurs politiques : plus le pouvoir économique de ces acteurs a augmenté, plus leur pouvoir politique s'est accentué. Les géants du numérique se placent en partenaires des gouvernements pour résoudre les problèmes dont ils sont les responsables. Pour les associations « Corporate Europe Observatory » et « LobbyControl », il s'agit désormais de la plus grande industrie de *lobbying* de l'Union Européenne[740].

256. Les dépenses exorbitantes. Lorsque l'Union européenne a souhaité réguler le secteur du numérique, les dépenses de *lobbying* des géants du numérique ont augmenté de façon drastique[741]. Les géants du numérique dépensent littéralement des millions en *lobbying* afin d'influencer les normes européennes. Les entreprises Apple, Facebook et Google ont respectivement dépensé plus de 6 millions d'euros en *lobbying* auprès de l'Europe en 2021[742]. Pour la première fois, un rapport établi par l'Observatoire des multinationales a été publié en décembre 2022 sur l'influence des géants américains en France et le rapport constate que les filiales françaises de ces multinationales ont multiplié par trois leurs dépenses en *lobbying* en

739 Pouillaude Sibylle, « "Attraper les GAFAM" ou le guichet unique en droit de la protection des données personnelles : fonctionnement, bilan et perspectives. », Revue des affaires européennes, n° 2023/1, pp. 127-151.

740 Corporate Europe Observatory, « The lobby network: Big Tech's web of influence in the EU Corporate Europe Observatory », disponible sur : https://corporateeurope.org/en/2021/08/lobby-network-big-techs-web-influence-eu.

741 Dechaux Delphine, « Comment Google et les Gafa ont tissé leurs réseaux d'influence à Bruxelles », Challenges, 2019, précisant que Google a multiplié par six ses dépenses de lobbying en Europe : « Pour avoir une première idée du lobbying des Gafa, il faut se pencher sur le "registre de la transparence", créé dès 1996 à Bruxelles. On peut y lire d'emblée la spectaculaire montée en puissance de Google. La firme de Mountain View emploie 15 lobbyistes, dont 9 à temps plein. Elle a multiplié par six ses dépenses de lobbying, passées de 1 à 6 millions d'euros entre 2011 et 2017. Et entre 2014 et 2018, ses lobbyistes ont assisté à 211 réunions avec la Commission européenne. », disponible en ligne.

742 Gaudiat Tristian, « Lobbying : les Big Tech dépensent des millions en Europe », Statista, disponible en ligne.

France depuis 2017 en déclarant plus de 4 millions en 2021[743]. Selon les associations, les géants américains de la technologie dépensent plus que tous les autres secteurs. À cette fin, ils embauchent le plus grand nombre de consultants en *lobbying*[744].

257. Pratiques de « porte tournante ». De fait, il existe une réelle problématique de « portes tambour[745] » ou « porte tournante », phénomène intensifié par les GAFAM[746]. Les géants du numérique n'hésitent pas à embaucher des fonctionnaires européens pour la défense de leurs propres intérêts. En droit, il s'agit du délit de pantouflage, désignant le passage pour un agent du secteur public vers le secteur privé[747] et les avantages pour les entreprises sont nombreux tels que la connaissance des rouages de l'administration, l'avancement des dossiers, des carnets d'adresses pour obtenir des contacts formels ou informels, etc.[748]. Le rapport « The lobby network : Big Tech's web of influence in the EU » estime que 70% des *lobbyistes* de Google et Facebook ont travaillé dans des institutions publiques au niveau national ou européen. Pour autant, il existe un risque de conflits d'intérêts permettant à ces entreprises de bénéficier d'une certaine complaisance[749].

---

743 Pignatelli Chiara et Petitjean Olivier, « GAFAM Nation. La toile d'influence des géants du web en France », Rapport, 2022.

744 Corporate Europe Observatory, *op. cit*., « En 2019 et 2020, Google, Apple, Amazon, Facebook et Microsoft et Qualcomm ont embauché le plus de consultants en lobbying. Ceux-ci comprenaient Fleishman-Hillard, EU-Strategy et FTI Consulting. Google reste en tête en dépensant 1,28 million d'euros pour 12 conseils, soit près d'un quart du budget total de lobbying de l'entreprise ».

745 Définition de la porte tambour : « phénomène de rotation de personnel entre un rôle de législateur et régulateur d'une part et un poste dans l'industrie affecté par ces mêmes législation et régulation (donc avec suspicion de conflit d'intérêt) d'autre part. Dans certains cas ces rôles sont assumés séquentiellement, mais dans certaines circonstances ils peuvent être assumés en même temps. Les analystes politiques pensent qu'une relation malsaine peut se développer entre le secteur privé et le gouvernement, basé sur l'allocation de privilèges réciproques au détriment de l'intérêt de la nation », en ligne disponible sur https://fr.wikipedia.org/wiki/Porte_tambour_(politique).

746 Selon Transparency International, entre 2009 et 2018, Google a engagé vingt-trois salariés qui travaillaient auparavant pour l'Union Européenne Onze d'entre eux y représentent maintenant les intérêts de l'entreprise, ce qui illustre bien le phénomène de porte tournante au sein des institutions européennes.

747 L'incrimination définie à l'article 432-13 du Code pénal est punie d'une peine de trois ans d'emprisonnement et d'une amende de 200 000 € ; Lasserre Capdeville Jérôme, « Le délit de "pantouflage" » AJCT, 2011, 395 : « Il serait tentant pour un agent public, chargé de contrôler une entreprise privée, d'avantager cette dernière, sachant que celle-ci a pour souhait de le recruter à brève échéance ».

748 Pignatelli Chiara et Petitjean Olivier, *op. cit*.

749 Vergnolle Suzanne, *L'effectivité de la protection des personnes par le droit des données à caractère personnel*, éd. Larcier, 2022, p. 399 : « De manière surprenante, la CNIL valorise ces situations en considérant que cette mobilité contribue "à la bonne diffusion de la culture de la protection des données". Pourtant, de telles pratiques risquent d'engendrer des risques de partialité, voire des conflits d'intérêts, pour les agents de service. En effet, dès lors qu'ils ont le pouvoir d'orienter les contrôles, d'y participer et d'en

258. L'exemple de Fiona Scott Morton. À titre d'illustration, la nomination de Fiona Scott Morton à la Commission européenne le 11 juillet 2023 a fait l'objet de nombreuses pressions. Elle avait été nommée au poste d'économiste au sein de la direction générale de la concurrence de la Commission européenne. Néanmoins, Fiona Scott Morton est une ancienne *lobbyiste* américaine de certains GAFAM. La nomination de cette ancienne consultante est une illustration probante du conflit d'intérêts en présence[750]. Il s'agit d'une personne refusant la dissolution des acteurs du numérique ou encore relayant la défense des consommateurs au second plan. Par conséquent, à la suite des nombreuses réticences et critiques lors de la diffusion de sa nomination, l'ancienne lobbyiste a fini par renoncer à ce poste[751].

2. L'influence incontestable des GAFAM

259. Influence des GAFAM. L'expansion du montant dépensé en *lobbying* par les géants du numérique démontre la puissance de ces multinationales. Afin d'illustrer l'influence des GAFAM sur l'élaboration des normes, il est possible de constater quelques exemples lors de l'adoption récente de certains règlements. Au sujet du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, il est d'usage que les articles de doctrine évoquent dans leur introduction « l'intense *lobbying* » exercé pour ce règlement[752]. Le règlement a fait l'objet de 4471 projets d'amendements et les

établir les rapports, ne risquent-ils pas d'être tentés d'être moins rigoureux à l'occasion des contrôles d'entreprises dans lesquelles ils souhaiteraient ensuite être recrutés ? ».

[750] Le Monde, « L'ex-lobbyiste américaine « Fiona Scott Morton est un cheval de Troie pour Big Tech » à la Commission européenne », 17 juillet 2023.

[751] Le Monde, « Fiona Scott Morton renonce à occuper le poste d'économiste en chef de la direction de la concurrence de la Commission européenne », 19 juillet 2023.

[752] Castets-Renard Céline, *Droit du marché unique numérique et intelligence artificielle*, éd. Bruylant, 2020, p. 22 : « Le marché européen attire les GAFAM (Google, Apple, Facebook, Amazon, Microsoft) et les hommes politiques européens n'ont de cesse de dénoncer le lobbying sans précédent exercé à Bruxelles par ces grandes entreprises américaines, comme on a pu le constater lors de l'adoption du règlement européen 2016/679/UE sur la protection des données personnelles dit "RGPD" qui fit l'objet de plus de 4000 amendements et moult rebondissements lors des débats parlementaires » ; Martial-Braz Nathalie, « Le champ d'application du RGPD » *in* Bensamoun Alexandra, Bertrand Brunessen et Anca Ailincail Mihaela et Martial-Braz Nathalie (dir.), *Le règlement général sur la protection des données: aspects institutionnels et matériels*, éd. Mare & Martin, 2020, p. 20 : « L'adoption du RGPD ne s'est toutefois par faite sans mal, et si le principe de son existence a été vite acquis, son contenu a fait l'objet d'un très long processus d'adoption, d'autant plus long qu'il a été perturbé par un lobbying extrêmement intense. Entre la proposition faite en janvier 2012 et l'adoption définitive du Paquet données le 27 avril 2016 se sont écoulées quatre années de discussions et d'atermoiements qui ont contribué à l'adoption d'un texte qui ne peut être que de compromis. ».

négociations ont duré 4 ans. En effet, les grands acteurs du numérique s'affranchissaient majoritairement des règles concernant la protection des données à caractère personnel de leurs utilisateurs, avec des conditions générales illisibles ou encore des transferts de données non consentis et étaient de ce fait hostiles à une réglementation uniforme au sein de l'Union Européenne. Des documents internes ont confirmé l'élaboration d'une campagne autour du règlement sur la protection des données afin de l'influencer, étant perçu comme une « menace critique » pour les activités de Facebook[753]. Pire encore, l'ancien député Jean-Marie Cavada évoque expressément des « menaces terribles » de la part des géants du numérique lors des négociations sur la directive des droits d'auteurs et droits voisins du 17 avril 2019[754]. Il y décrit une campagne mensongère, le paiement de sommes d'argent afin de « gêner » les négociations ou encore des menaces implicites[755]. Les menaces de ces acteurs ont pour dessein d'insérer des brèches dans les projets de règlements.

260. Insertion de « brèches ». En effet, les brèches vont leur permettre de maintenir une certaine liberté dans le traitement des données à caractère personnel. À titre d'illustration, Google a appelé « au maintien de la viabilité de la règle des intérêts légitimes » afin de « permettre aux entreprises de traiter les informations en dehors du consentement explicite grâce à la transparence et à un contrôle de l'utilisateur accrus[756] ». Ainsi, par la justification d'un certain « intérêt légitime », les acteurs du numérique vont pouvoir traiter des données à caractère personnel lorsqu'ils ont un intérêt dit « légitime » par exemple économique, dans le cas où ce dernier ne porte pas atteinte aux personnes concernées[757]. En réalité, les géants du numérique traitent un grand nombre de données sous couvert d'un motif économique, vidant de sa substance le principe de protection des données à caractère personnel. La base légale - voire la brèche - de l'intérêt légitime permet donc aux géants du numérique de traiter des données à caractère personnel en toute légalité.

---

[753] Le Monde, « De nouveaux documents détaillent le lobbying de Facebook », 4 mars 2019 : « De nouveaux documents, dont le contenu a été révélé dimanche 3 mars par le Guardian et Computer Weekly, détaillent les pratiques de Facebook en matière de lobbying. Vraisemblablement issus des documents juridiques liés à un procès intenté à Facebook en Californie par une start-up, Six4Three, les documents comprennent plusieurs mémorandums internes de Facebook et éclairent les rapports du réseau social avec plusieurs chefs de gouvernement et avec l'Union européenne. ».

[754] Directive (UE) 2019/790 du Parlement européen et du Conseil du 17 avril 2019 sur le droit d'auteur et les droits voisins dans le marché unique numérique et modifiant les directives 96/9/CE et 2001/29/CE.

[755] Cavada Jean-Marie, « Rencontre avec Jean-Marie Cavada - Big Ideas Big Names in IP », Podcast R2PI, CEIPI, 10 minutes 48, septembre 2023, disponible sur Spotify.

[756] Barron Andrew et Voss Gregory, *op. cit*.

[757] *Infra.*, n° 511.

261. Influence sur la Directive 2019/790 du Parlement européen et du Conseil du 17 avril 2019 sur le droit d'auteur et les droits voisins dans le marché unique numérique. Les intérêts économiques des acteurs du numérique peuvent également être mis en lien avec la directive 2019/790. L'un des objectifs de la directive était de favoriser la diffusion d'œuvres protégés par le droit d'auteur ou un droit voisin. Pour ce faire, plusieurs outils peuvent être sollicités dont les articles 3 et 4 concernant la fouille de données. Afin de faciliter cette fouille, les articles précités instituent des exceptions : l'une soumise à une finalité d'exercice « scientifique » et la seconde à aucune finalité. L'article 3 de la directive subordonne l'accès à un *data mining* établi « à des fins de recherche scientifique ». Les bénéficiaires sont les organismes de recherche ou les institutions du patrimoine culturel. Au contraire, l'article 4 subordonne cet accès à aucune finalité particulière, l'exception étant étendue à toutes les entités privées ou publiques[758]. Auparavant, au niveau national, la fouille de données était pourtant limitée à la recherche au sein de la Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique. La transposition de la directive a donc permis la reconnaissance de l'exception de fouille de données « quelle que soit la finalité de la fouille », conditionnée uniquement par un l'*opt-out* de l'auteur[759]. Le considérant 18 de la directive précise que l'exception de *data mining* peut permettre « l'élaboration de nouvelles applications ou technologies[760] ». Nul besoin d'expliciter quels sont les acteurs bénéficiaires de cette exception, dont l'influence est incontestable.

262. Influence sur le Règlement (UE) 2022/1925 du Parlement européen et du Conseil du 14 septembre 2022 relatif aux marchés contestables et équitables dans le secteur numérique (DMA) et Règlement (UE) 2022/2065 du 19 octobre 2022 du Parlement européen et du Conseil relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (DSA). Ensuite, lors des discussions autour des règlements sur les

[758] Bruguière Jean-Michel, *La directive droit d'auteur dans le marché unique numérique (2019/790)*, éd. Larcier, 2020, p. 26 : « Il est permis de se demander d'ailleurs si l'article 4 institue bien une exception puisqu'au final le propriétaire des bases de données convoitées pour le data mining peut écarter la fouille par un certain nombre d'opérations. L'exception de l'article 3 est bien obligatoire, celle de l'article 4 est finalement facultative. ».

[759] Martial-Braz Nathalie, « IA générative ou l'émergence de risques insoupçonnés pour la création ! », CCE, n° 6, juin 2023 : « Si la question des produits de l'intelligence artificielle se pose, la question des droits des auteurs à l'origine des contenus, désormais engloutis au rang de données par ces systèmes voraces et apprenants, est également au cœur des préoccupations des législateurs. ».

[760] Directive 2019/790 du Parlement européen et du Conseil du 17 avril 2019 sur le droit d'auteur et les droits voisins dans le marché unique numérique, considérant 18.

services et les marchés numériques, les dépenses de *lobbying* des géants du numérique ont explosé[761] et certains eurodéputés ont même déposé une plainte afin de dénoncer des pratiques de *lobbying* dissimulé[762]. De surcroît, des députés européens ont été victimes d'*astroturfing* ou encore de ciblage publicitaire agressif sur leurs réseaux sociaux[763]. L'*astroturfing* est une méthode de manipulation utilisée sur internet consistant à donner l'impression d'un phénomène de masse qui émerge de façon spontanée alors qu'en réalité, il a été créé de toutes pièces afin d'influencer l'opinion publique[764]. Pour lesdits règlements, les géants du numérique ont utilisé cette pratique déloyale en manipulant des organisations représentatives des citoyens et des petites entreprises. En outre, selon les associations précitées, sur les 271 rencontres pour discuter des règlements précités, 75% ont eu lieu avec les *lobbyistes* de l'industrie du numérique. Ces acteurs vont plaider qu'il serait plus opportun d'établir une approche au cas par cas en déplaçant le débat sur les plans techniques, qu'ils maîtrisent mieux que quiconque[765]. À titre d'illustration, le passage du seuil du chiffre d'affaires et de capitalisation boursière dans le règlement sur les marchés numériques de 6,5 millions[766] à 7,5 millions est assurément le fruit du *lobbying* de ces acteurs[767].

---

761 Lepilleur Sarah, « Le DSA-DMA fait bondir les dépenses de lobbying des Gafa à Bruxelles », sur Les Echos, publié le 31 août 2021.

762 Moutot Romain, « Lutte contre les pratiques déloyales des GAFAM : le DMA est publié ! », Dalloz Actualité, 16 novembre 2022 ; Les plaintes proviennent de Christel Schaldemose, rapporteure du Digital Service Act, René Repasi et Paul Tang, rapporteurs fictifs sur le Digital Markets Act.

763 Lepilleur Sarah, *op. cit.*

764Définition de l'astroturfing, disponible à l'adresse : https://www.lalanguefrancaise.com/dictionnaire/definition/astroturfing.

765 « GAFAM Nation. La toile d'influence des géants du web en France », *op. cit*., p. 24.

766 Proposition de Règlement du parlement européen et du conseil relatif aux marchés contestables et équitables dans le secteur numérique (législation sur les marchés numériques), article 3 : « Un fournisseur de services de plateforme essentiels est réputé satisfaire : (a) à l'exigence du paragraphe 1, point a), si l'entreprise à laquelle il appartient a réalisé un chiffre d'affaires annuel dans l'EEE supérieur ou égal à 6 500 000 000 EUR au cours des trois derniers exercices, ou si la capitalisation boursière moyenne ou la juste valeur marchande équivalente de l'entreprise à laquelle il appartient a atteint au moins 65 000 000 000 EUR au cours du dernier exercice, et qu'il fournit un service de plateforme essentiel dans au moins trois États membres. ».

767 Règlement (UE) 2022/1925 du parlement européen et du conseil du 14 septembre 2022 relatif aux marchés contestables et équitables dans le secteur numérique et modifiant les directives (UE) 2019/1937 et (UE) 2020/1828 (règlement sur les marchés numériques), article 3 : « Une entreprise est réputée satisfaire aux exigences respectives du paragraphe 1: a) en ce qui concerne le paragraphe 1, point a), si elle a réalisé un chiffre d'affaires annuel dans l'Union supérieur ou égal à 7,5 milliards d'euros au cours de chacun des trois derniers exercices, ou si sa capitalisation boursière moyenne ou sa juste valeur marchande équivalente a atteint au moins 75 milliards d'euros au cours du dernier exercice, et qu'elle fournit le même service de plateforme essentiel dans au moins trois États membres. ».

263. Influence sur le règlement e-Privacy[768]. Initialement, le règlement e-Privacy devait entrer en vigueur concomitamment avec le RGPD. À ce jour, soit 8 ans après l'entrée en vigueur du règlement sur la protection des données à caractère personnel, le règlement e-Privacy n'est toujours pas en vigueur[769]. Ainsi, entre la proposition et les négociations du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, un certain nombre d'années se sont écoulées. Le conflit porte nécessairement sur l'objet même du règlement étant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques. L'un des objectifs du règlement est de renforcer l'encadrement juridique sur les *cookies* : la pratique de la traçabilité de la navigation des utilisateurs permet aux plateformes de vendre les données afin que les annonceurs puissent proposer la publicité ciblée. Or, c'est principalement sur cette offre que repose le modèle d'affaires de la majorité des plateformes[770]. Ainsi, à l'instar des règlements précités, les entreprises du numérique pratiquent un *lobbying* intense, qualifié de « déraisonnable et grave »[771], voire « ignoble », toujours selon les mots de Jean-Marie Cavada[772].

[768] Proposition de règlement du parlement européen et du conseil concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques et abrogeant la directive 2002/58/CE (règlement « vie privée et communications électroniques »), COM/2017/010 final.

[769] En France, la CNIL a anticipé le règlement et oblige, depuis le 1er avril 2021, tous les sites internet à suivre l'article 82 de la LIL qui permet de refuser aux internautes aussi facilement qu'ils peuvent accepter l'utilisation des cookies destinés au traçage publicitaire. De surcroît, un silence doit être interprété comme un refus ; Face à l'intense lobbying des GAFAM sur les normes européennes, plusieurs groupes tels que LobbyControl, Corporate Europe Observatory et plusieurs députés européens ont décidé d'ouvrir une hotline « LobbyLeaks » afin de signaler les pratiques douteuses. Le site garantit l'anonymat et l'intracabilité des contributions. Le site permettra de collecter les données sur les pratiques douteuses qui affectent l'élaboration des normes en matière de régulation du numérique. La collecte de données servira à renforcer les dossiers de plainte déposé au registre de transparence.

[770] Selon The Developers Alliance, le manque à gagner pour les entreprises serait de 640 milliards d'euros de chiffre d'affaires.

[771] Selon le député Jan Phillipp Albrecht, Facebook, Google, Microsoft, SAP ou IBM sont tous entrés en contact avec des officiels de la Commission européenne, selon la base de données de Transparency International UE.

[772] « Réforme européenne du droit d'auteur : Cavada dénonce le lobbying "ignoble" des Gafa », sur France Inter, publié le 26 mars 2019, disponible sur : https://www.radiofrance.fr/franceinter/reforme-europeenne-du-droit-d-auteur-cavada-denonce-le-lobbying-ignoble-des-gafa-2155383.

264. Conclusion de la section. Tous les domaines du droit sont impactés par l'essor des données. Les initiatives législatives se succèdent ces dernières années à un rythme effréné et de nouveaux projets sont encore en cours de discussion afin de construire un cadre normatif pour les données. En effet, la multiplication des normes est influencée par des intérêts divergents. Il s'agit de développer les intérêts économiques tout en protégeant les individus et depuis peu, le climat.

Les plateformes participent cette construction du cadre afin d'impacter le contenu des normes. Leur intérêt est de s'affranchir des normes européennes afin de pouvoir continuer de bâtir leur empire sur les données. Ils ont développé leur propre marché, leurs propres règles. En développant le marché de l'intelligence artificielle, les plateformes se retrouvent parfois dépassées par leurs propres systèmes. Ainsi, malgré la pluralité de normes, de droit dur ou de droit souple, l'applicabilité des normes va dépendre de la volonté des géants du numérique.

De surcroît, lorsqu'il n'est pas possible de s'affranchir des normes européennes et pour leur image de marque, les géants du numérique vont investir dans le *lobbying* en faisant valoir leurs propres intérêts. La corrélation entre la réglementation européenne sur les données et les dépenses en *lobbying* des GAFAM est alarmante, leur unique intérêt étant d'intégrer des brèches dans les normes régissant un domaine qu'ils ont créé. À force d'avoir intégré les acteurs privés dans l'élaboration des normes sur les données, ils deviennent les seuls susceptibles de comprendre les règles établies et surtout, de quelle manière les contourner.

265. Conclusion du chapitre. Depuis les débuts de l'élaboration du marché unique numérique, l'Union européenne a légiféré en prenant en compte des objectifs antagonistes, c'est-à-dire l'ouverture des données à caractère non personnel et la protection des données à caractère non personnel. L'Union européenne souhaite limiter l'exploitation abusive des données à caractère personnel des utilisateurs par les géants du numérique. En parallèle, elle souhaite libérer les flux de données à caractère non personnel en supprimant les exigences de localisation des données à caractère non personnel. La libéralisation des flux permettrait de désamorcer la concentration abusive des données à caractère non personnel par les mêmes acteurs.

D'une façon inévitable, la prise en compte d'objectifs antagonistes a entraîné l'élaboration de régimes antagonistes. Le règlement sur la protection des données à caractère personnel permet aux individus de reprendre - ou prendre - le contrôle sur leurs données. Lorsque les données sont qualifiées de personnelles, le régime de protection s'applique. En revanche, dans le dessein de libérer le potentiel des données à caractère non personnel, dès lors qu'une donnée est qualifiée de non personnelle, les flux seront libérés afin de pouvoir réutiliser et accéder à ces données. Pour les données publiques, une politique d'*open data* est en construction afin d'exploiter le potentiel économique de ces données. En réalité, les régimes antagonistes ne permettent pas de trouver un équilibre et l'Union européenne semble prioriser l'ouverture des données à caractère non personnel au regard des récents règlements.

En pratique, les géants du numérique ne sont pas réellement enclins à libérer leur masse de données, ni à restreindre leurs pratiques d'exploitation des données à caractère personnel. Ainsi, ils exercent un *lobbying* afin de défendre leurs propres intérêts et, *in fine,* d'influencer l'élaboration des normes. L'influence est d'abord pédagogique puisqu'ils sont les seuls à avoir la réelle maîtrise de leurs outils. Ils partagent leurs connaissances avec le législateur afin d'élaborer des normes adéquates à leurs usages. Néanmoins, la pédagogie n'est pas leur principale qualité. En réalité, ils prônent l'autorégulation afin d'échapper à des règles trop contraignantes. Lorsque le législateur légifère par le droit dur, ils dépensent des sommes astronomiques en *lobbying*.

La prise en compte des objectifs et intérêts antinomiques dans l'élaboration du cadre normatif des données a entraîné un régime complexe et diversifié. Au stade de la réglementation sur les données à caractère personnel et du règlement sur le libre flux des données à caractère non

personnel, les géants du numérique ont réussi à imprégner leur influence dans les textes. Le bilan est décevant et leur influence en croissance. Dès lors, la réglementation apparaît comme antagoniste et ambivalente. Ainsi, l'Union européenne a décidé de renforcer les obligations des acteurs du numérique afin de rendre effective l'ouverture des données. Pour ce faire, elle a dévoilé une « réglementation concurrentielle » des données.

Chapitre 2 : L'émergence d'un cadre concurrentiel pour les données

266. Stratégie d'ouverture des données. À la suite du bilan décevant du Règlement (UE) 2018/1807 établissant un cadre applicable au libre flux des données à caractère non personnel, l'Union européenne réitère et consolide sa stratégie d'ouverture des données. Désormais, le législateur européen cible les géants du numérique - sans directement les nommer - afin de lutter contre l'accumulation massive des données (**Section 1**). En parallèle, afin d'exploiter le potentiel des données à caractère non personnel, l'Union européenne retient une approche globale pour favoriser le partage des données. Il s'agit désormais de contrer l'influence des acteurs du numérique en développant un modèle alternatif voire antinomique à leur fonctionnement : une gouvernance de confiance pour les données. Le modèle de partage des données est fondé sur la confiance et l'altruisme, modèle qui nous semble chimérique en pratique (**Section 2**).

Section 1 : Le recours à une réglementation ciblée contre l'accumulation massive des données

267. Réglementation ciblée. Afin de contrer l'accès monopolistique des données par certains acteurs du numérique, le Règlement (UE) 2022/1925 du Parlement européen et du Conseil du 14 septembre 2022 relatif aux marchés contestables et équitables dans le secteur numérique est entré en vigueur le 6 mars 2024 afin de mettre en place une réglementation contre l'accès asymétrique aux données (I). De surcroît, le contrôle des utilisateurs sur leurs données et la transparence des plateformes sont renforcés par le Règlement (UE) 2022/2065 du 19 octobre 2022 du Parlement européen et du Conseil relatif à un marché unique des services numériques (II).

I. Une réglementation contre l'accès asymétrique aux données

268. Approche ciblée. Durant les dernières années, le recours au droit de la concurrence n'a pas permis de lutter contre l'accès monopolistique des géants du numérique sur la masse de données. Dès lors, l'adaptation de l'approche traditionnelle du droit de la concurrence était inéluctable (B) afin d'établir une approche ciblée contre l'accès asymétrique des données (A).

A) L'adaptation de l'approche traditionnelle du droit de la concurrence

269. Limites du droit de la concurrence. Dans les faits, les géants du numérique détiennent une position dominante, difficilement caractérisable en droit de la concurrence en raison du caractère disruptif de leurs activités. Ainsi, le droit de la concurrence s'est révélé inadéquat afin d'empêcher leur développement monopolistique sur la détention de données (1). Désormais, l'Union européenne cible spécifiquement les GAFAM (2).

1. L'inadéquation du droit de la concurrence au marché des données

270. L'approche traditionnelle du droit de la concurrence. Le droit de la concurrence a pour aspiration de maintenir une libre concurrence entre les différents acteurs sur un marché. Lorsqu'une entreprise adopte un comportement visant à éliminer ou contraindre un concurrent de s'établir sur ce marché ou un marché connexe, l'entreprise est caractérisée par un abus de position dominante. Ce type de comportement est prohibé par l'article 420-2 du code de commerce[773]. Dans le cas d'affectation du commerce intra-communautaire, la pratique relève du droit de l'Union européenne et est également prohibée par l'article 102 du TFUE[774]. En droit de la concurrence, plusieurs conditions doivent être réunies afin de caractériser un abus de position dominante[775]. Tout d'abord, l'entreprise doit détenir une position dominante sur un marché déterminé dit marché pertinent : cette dernière doit l'exploiter de manière abusive et cela doit avoir un effet restrictif de concurrence. En effet, le simple fait pour une entreprise de détenir une forte part de marché ne permet pas de conclure à un abus de position dominante.

[773] Code de commerce, article 420-2 : « Est prohibée, dans les conditions prévues à l'article L. 420-1, l'exploitation abusive par une entreprise ou un groupe d'entreprises d'une position dominante sur le marché intérieur ou une partie substantielle de celui-ci. Ces abus peuvent notamment consister en refus de vente, en ventes liées ou en conditions de vente discriminatoires ainsi que dans la rupture de relations commerciales établies, au seul motif que le partenaire refuse de se soumettre à des conditions commerciales injustifiées. ».

[774] Traité sur le fonctionnement de l'Union européenne, article 102 : « Est incompatible avec le marché intérieur et interdit, dans la mesure où le commerce entre États membres est susceptible d'en être affecté, le fait pour une ou plusieurs entreprises d'exploiter de façon abusive une position dominante sur le marché intérieur ou dans une partie substantielle de celui-ci. ».

[775] Définition de la position dominante : « La position dominante concerne une position de puissance économique détenue par une entreprise qui lui donne le pouvoir de faire obstacle au maintien d'une concurrence effective sur le marché en cause, en lui fournissant la possibilité de comportements indépendants dans une mesure appréciable vis à vis de ses concurrents, de ses clients et, finalement, des consommateurs. ». (CJUE 14 février 1978, United Brands et United Brands Continental BV/Commission, 27/76, point 65).

En revanche, lorsque l'entreprise détient une avance technologique lui permettant d'augmenter ses prix sans craindre une perte de clientèle, l'abus peut être caractérisé.

271. Les limites du droit de la concurrence. En apparence, le droit de la concurrence pourrait s'appliquer aux géants du numérique au regard de leur position dominante, voire monopolistique sur les données. Néanmoins, la délimitation du marché pertinent s'avère complexe pour les pratiques des géants du numérique, particulièrement avec l'usage des modèles gratuits[776]. En effet, l'absence de prix des services numériques met à mal l'application du droit classique de la concurrence[777]. Par ailleurs, le droit de la concurrence s'applique *ex post* et nécessite des enquêtes approfondies. La démonstration de l'effet restrictif consiste à mesurer les effets économiques néfastes d'une pratique et cela nécessite alors la collecte d'une certaine quantité d'information avant de pouvoir qualifier la pratique d'abusive[778].

En réalité, les faits sont généralement trop complexes rendant les abus de position dominante difficiles à caractériser[779]. Les pratiques des géants du numérique sont souvent opaques, rendant difficile la collecte d'informations pertinentes. L'accès asymétrique à ces informations et la dimension technique de leurs pratiques ont permis à ces acteurs de se développer sans être sanctionnés sur le terrain de la concurrence[780]. De fait, ces acteurs ont pu verrouiller leurs marchés disruptifs aux potentiels concurrents émergents[781].

---

[776] Chagny Muriel, « La régulation des plateformes numérique par le droit de la concurrence », Revue Lamy de la concurrence, n° 129, 1er juillet 2023.

[777] De Streel Alexandre « Les données, l'innovation et le droit des concentrations », *in* De Terwangne Cécile, Degrave Elise, Queck Robert, Dusollier Séverine (dir.), *Law, norms and freedoms in cyberspace. Droit, normes et libertés dans le cybermonde. Liber amicorum Yves Poullet*, éd. Larcier, 2018, p. 113.

[778] Amaro Rafael, « La régulation concurrentielle de la donnée. Par le droit de la concurrence et au-delà du droit de la concurrence », *in* Bruguière Jean-Michel, *L'émergence d'un droit des données*, éd. Dalloz, 2023, p. 129.

[779] Règlement (UE) 2022/1925 du parlement européen et du conseil du 14 septembre 2022 relatif aux marchés contestables et équitables dans le secteur numérique, considérant 5 : « Il s'ensuit que les processus du marché sont souvent incapables de garantir des résultats économiques équitables en ce qui concerne les services de plateforme essentiels. Si les articles 101 et 102 du traité sur le fonctionnement de l'Union européenne s'appliquent au comportement des contrôleurs d'accès, le champ d'application de ces dispositions se limite à certains cas de pouvoir de marché, par exemple la position dominante sur certains marchés et le comportement anticoncurrentiel, et l'application intervient ex post et requiert une enquête approfondie, au cas par cas, sur des faits souvent très complexes. En outre, le droit existant de l'Union ne répond pas, ou pas efficacement, aux entraves au bon fonctionnement du marché intérieur dues au comportement de contrôleurs d'accès qui n'occupent pas nécessairement de position dominante au sens du droit de la concurrence. ».

[780] Lequette Suzanne, *Droit du numérique,* éd. LGDJ, 2024, p. 753.

[781] Favro Karine et Zolynski Célia, « DSA, DMA, l'Europe encore au milieu du gué », Dalloz IP/IT, 2021, p. 217.

272. Règlement (UE) 2022/1925 du Parlement européen et du Conseil du 14 septembre 2022 relatif aux marchés contestables et équitables dans le secteur numérique (DMA). Afin de contrer les limites du droit de la concurrence et de s'adapter à ces nouveaux marchés, le règlement sur les marchés numériques vient compléter les dispositifs de ce cadre normatif[782]. Selon l'article 1 paragraphe 6, le règlement s'applique sans préjudice du droit des pratiques anticoncurrentielles. Ainsi, sur le fondement de l'article 114 du TFUE, le règlement poursuit l'objectif d'établir des règles harmonisées visant à garantir aux entreprises la contestabilité et l'équité des marchés dans le secteur du numérique[783].

Dans l'intention d'adapter le droit de la concurrence aux nouveaux acteurs, le règlement sur les marchés numériques traite inégalement les contrôleurs d'accès afin de rétablir une concurrence loyale entre les acteurs du numérique. Au regard de leur poids économique, il était nécessaire de créer une catégorie spécifique pour ces acteurs. À cette fin, le texte proscrit certains comportements néfastes afin de réduire leur position quasi monopolistique sur le marché des services numériques. Lorsque les règlements traitent indifféremment les acteurs du numérique, ce sont les petites et moyennes entreprises qui sont pénalisées. Les géants du numérique détiennent les moyens techniques et financiers de respecter les règlements, et sont en position de force vis-à-vis des autres entreprises. Surtout, ce sont principalement leurs pratiques qui sont les plus néfastes pour les individus.

[782] Vandenhende Elodie, « Application du DMA par les autorités de concurrence et le juge de droit commun », Revue Lamy de la concurrence, n° 129, 1er juillet 2023 : « Le DMA aura un rôle complémentaire mais distinct du droit de la concurrence » ; Règlement (UE) 2022/1925 du parlement européen et du conseil du 14 septembre 2022 relatif aux marchés contestables et équitables dans le secteur numérique, considérant 10 : « Dans le même temps, puisque le présent règlement vise à compléter l'application du droit de la concurrence, il devrait s'appliquer, sans préjudice des articles 101 et 102 du traité sur le fonctionnement de l'Union européenne, aux règles de concurrence nationales correspondantes et aux autres règles de concurrence nationales relatives au comportement unilatéral, qui reposent sur une évaluation individualisée des positions et du comportement sur le marché, y compris les effets réels ou éventuels ainsi que la portée précise du comportement interdit, et qui prévoient la possibilité pour les entreprises de justifier objectivement le comportement en question par des motifs d'efficience, ainsi qu'aux règles nationales concernant le contrôle des concentrations. ».

[783] Règlement (UE) 2022/1925 du parlement européen et du conseil du 14 septembre 2022 relatif aux marchés contestables et équitables dans le secteur numérique, article 1, point 1.

2. L'émergence d'une réglementation concurrentielle de la donnée

273. Possession monopolistique des données. L'un des principaux comportements néfastes des géants du numérique se traduit par la possession monopolistique des données à caractère personnel de leurs utilisateurs. Les géants du numérique ont pendant longtemps collecté les données à caractère personnel sans se préoccuper de la protection des utilisateurs et ils détiennent une grande masse de données collectée sur leurs services et les services tiers[784]. La possession monopolistique de données leur a permis de développer de nouveaux services et de collecter toujours plus de données[785], aboutissant à une position de force face à de nouveaux entrants[786]. À ce jour, le poids économique d'une entreprise n'est plus exclusivement défini en termes de chiffres d'affaires mais également d'accès aux données[787] : l'apport concurrentiel de la donnée n'est plus à démontrer pour les entreprises[788]. Finalement, aucun acteur émergent ne pourra détenir la masse de données des acteurs entrés lors de l'arrivée d'internet.

274. Réglementation concurrentielle de la donnée. Ainsi, le règlement sur les marchés numérique complète le droit de la concurrence par une régulation concurrentielle de la donnée : la donnée est désormais considérée comme un actif concurrentiel conférant un important pouvoir de marché. La possession massive de données peut produire des effets anticoncurrentiels lorsque la plateforme centralise les données et devient un partenaire incontournable pour les autres acteurs. De fait, la plateforme détient le pouvoir de restreindre l'accès au marché aux opérateurs tiers dans le secteur de la publicité en ligne mais également

784 Poullet Yves, « Cinq ans après : le RGPD et les défis du profilage à l'heure de l'intelligence artificielle », Revue des affaires européennes, numéro 1, p. 88 : « L'utilisation de systèmes d'information fondés sur l'IA modifie les modalités et la portée du profilage de manière essentielle et ce pour diverses raisons. La première tient au fait que les systèmes d'information actuels par leur interconnexion et leur ubiquité permettent d'élargir - et ce de manière exponentielle - le nombre de données collectées et traitées. Si hier, les capacités de stockage et de communication des données étaient limitées, aujourd'hui, d'une part ces capacités sont devenues quasiment infinies comme le démontre le phénomène des mégadonnées et, d'autre part, l'internet des objets connectés. »

785 Behar-Touchais Martine, « Intelligence artificielle et concurrence », *in* Bensamoun Alexandra et Loiseau Grégoire (dir.), *Droit de l'intelligence artificielle*, éd. LGDJ, 2022, p. 203.

786 Guichardaz Rémy et Pénin Julien, « L'économie de la réutilisation des données (non personnelles) », Dalloz IP/IT, 2020, p. 218.

787 Laneret Nathalie et Knittel Rachel Baudequin Anne, « Protection des données à caractère personnel : quand le droit de la concurrence s'en mêle », Dossier IP/IT, p. 619.

788 Viangalli Francois, « Le concept de données en droit du numérique. Essai de définition », Revue Lamy Droit de l'Immatériel, n° 202, 1er avril 2023, p. 3 : « Sous cet angle [avantage concurrentiel], la donnée est une information privilégiée dont la détention et l'usage sont de nature à renforcer une position sur le marché, et qui relève par conséquent du droit de la concurrence. ».

contre d'autres acteurs du numérique concurrents[789]. De surcroît, elle va pouvoir étendre ses activités à de nouveaux secteurs grâce à la détention de la masse de données et cette extension lui permet d'accroître son avantage concurrentiel mais surtout, de maintenir l'utilisateur dans son propre écosystème[790]. Les pratiques des GAFAM ne sont pas concurrentielles et ces acteurs ont exploité les données grâce à l'absence de cadre réellement contraignant jusqu'à présent. Même en ouvrant les données sur le marché européen, les géants du numérique disposent d'un monopole qui ne peut pas être concurrencé pour le moment et d'une avance technologique sur les données pour le moment inégalable. Toutefois, l'entrée en vigueur du règlement sur les marchés numériques était espérée afin de ralentir leur position et d'ouvrir le marché aux concurrents.

Ainsi, le règlement sur les marchés numériques a pour objectif de limiter le pouvoir de marché de ces acteurs qui repose sur la détention de données. Pour ce faire, le règlement qualifie d'avantage concurrentiel « les effets de réseau et les avantages tirés des données, en particulier en ce qui concerne l'accès aux données à caractère personnel et non personnel et la collecte de ces données par ladite entreprise, ou les capacités d'analyse de cette dernière[791] ». Il s'agit de rétablir une concurrence loyale entre les différents acteurs en restreignant l'accès asymétrique de ces données.

B) La nouvelle approche ciblée contre l'accès asymétrique des données

275. Qualification des acteurs. Afin de contraindre les géants du numérique spécifiquement, l'Union européenne a fait le choix de cibler les acteurs selon des critères de taille (1). Les acteurs qualifiés de contrôleurs d'accès seront désormais soumis à une interdiction de combiner et de croiser les données qu'ils détiennent afin qu'ils ne puissent pas davantage renforcer leur position monopolistique en matière de détention de données à caractère personnel (2).

[789] Marty Frédéric, « L'économie de la donnée », *in* Bruguière Jean-Michel, *L'émergence d'un droit des données*, éd. Dalloz, 2023, p. 27.
[790] Amaro Rafael, *op. cit*., qui cite la première affaire Google Search Shopping du 17 juin 2017, COMP/39.740, confirmé par le Tribunal Union européenne, 10 novembre 2021, aff. T-612/17.
[791] Règlement (UE) 2022/1925 du Parlement européen et du Conseil du 14 septembre 2022 relatif aux marchés contestables et équitables dans le secteur numérique, article 3.8 c).

1. La qualification asymétrique des contrôleurs d'accès

276. Qualification de contrôleurs d'accès. Un « *gatekeeper* », autrement dit un contrôleur d'accès, est défini comme une entreprise fournissant des services de plateforme essentiels. De fait, le contrôleur d'accès est une entreprise susceptible de contrôler l'accès au marché numérique[792]. La qualification de contrôleur d'accès ouvre une nouvelle catégorie d'opérateurs, qui cible - sans les nommer - les géants du numérique. En 2019, le tribunal de commerce de Paris avait déjà qualifié Amazon de « quasi-gardien de l'accès aux marchés et aux consommateurs »[793]. Afin de s'adapter aux particularités de ces plateformes, le règlement a adopté des règles spécifiques[794]. Tout d'abord, le règlement propose trois critères cumulatifs pour qualifier une entreprise de contrôleur d'accès : le poids de l'entreprise sur le marché intérieur, le service essentiel fourni constituant un point d'accès majeur permettant aux entreprises utilisatrices d'atteindre leurs utilisateurs finaux et la position solide et durable de cette entreprise[795]. Ainsi, le règlement vise les entreprises qui détiennent des « avantages liés aux données[796] » ou encore qui ont « accès à de vastes quantités de données[797] », contrôlant le marché grâce à la détention et l'accès aux données[798].

---

[792] Bouckaert Colette, « Le règlement DMA : un texte novateur avec des faiblesses », sur iDFRights, en ligne, publié le 25 avril 2022, disponible sur https://idfrights.org.

[793] Tribunal de commerce de Paris, 2 décembre 2019, n°2017050625.

[794] Petel Antoine, « Quel bilan normatif pour l'Europe numérique ? », LexisNexis, Europe, n°5, mai 2024.

[795] Les critères cumulatifs sont complétés par des présomptions simples reposant sur des seuils quantitatifs. Tout d'abord, la présomption du poids de l'entreprise sur le marché intérieur s'observe grâce à un critère financier et un critère territorial. Le critère financier s'établit à travers son chiffre d'affaires annuel dans l'Union qui doit être supérieur ou égal à 7,5 milliards d'euros au cours de chacun des trois derniers exercices, ou si sa capitalisation boursière moyenne ou sa juste valeur marchante équivalente a atteint au moins 75 milliards d'euros au cours du dernier exercice. Quant au critère territorial, le service de plateforme essentiel doit être fourni dans au moins trois États membres. Dans un second temps, la présomption de l'existence d'un point d'accès majeur se calcule avec le nombre d'utilisateurs du service. Le service de plateforme doit avoir compté au cours du dernier exercice au moins 45 millions d'utilisateurs finaux actifs par mois établis ou situés dans l'Union et au moins 10 000 entreprises utilisatrices actives par an établies dans l'Union. Pour finir, le critère de stabilité est caractérisé lorsque le nombre d'utilisateurs est atteint au cours de chacun des trois derniers exercices.

[796] Règlement (UE) 2022/1925 du Parlement européen et du Conseil du 14 septembre 2022 relatif aux marchés contestables et équitables dans le secteur numérique, considérant 2.

[797] *Ibid.*, considérant 3.

[798] Favro Karine et Zolynski Célia, « DSA, DMA, l'Europe encore au milieu du gué », *op. cit*.

277. Désignation des contrôleurs d'accès. Le 5 septembre 2023, la Commission européenne a publié une première liste désignant six contrôleurs d'accès. Il s'agit de géants du numérique tels qu'Alphabet (Google), Amazon, Apple, Meta (Facebook) et Microsoft et du groupe chinois ByteDance, propriétaire de TikTok. Plus récemment, la société mère du site « Booking.com » a également été désignée[799]. Par conséquent, plus d'une vingtaine de services de plateformes essentiels fournis par ces contrôleurs d'accès ont été désignés[800]. De façon prévisible, certaines plateformes ont contesté leur désignation en tant que contrôleur d'accès : ByteDance pour sa plateforme TikTok[801] et Apple[802]. Quant à la société Meta, elle conteste l'intégration de ses services Messenger et Marketplace en tant que « services de plateformes essentiels »[803]. À l'instar de leurs pratiques de *lobbying*, les plateformes sont prêtes à tout pour ne pas respecter leurs obligations. Dès lors que les obligations a trait à leur matière première, c'est-à-dire les données, les géants du numérique contestent l'applicabilité des règles.

Néanmoins - à ce jour -, les contrôleurs d'accès précités sont en demeure de se mettre en conformité avec le règlement, par exemple sur l'interdiction de combiner les données à caractère personnel des utilisateurs sur leurs différents services.

2. L'interdiction de combinaison et de croisement des données à caractère personnel des utilisateurs

278. Interdiction de combinaison et de manipulation des données à caractère personnel. Afin de rétablir une concurrence loyale, le règlement sur le marché numérique interdit certaines pratiques de collecte et de manipulation de données aux contrôleurs d'accès. L'interdiction de ces pratiques va permettre de restreindre les effets réseaux et les avantages tirés des données par ces plateformes. Pour ce faire, l'article 5 paragraphe 2 établit plusieurs interdictions relatives à la combinaison des données à caractère personnel des utilisateurs.

[799] Décision du 13 mai 2024 par la Commission européenne.
[800] Il s'agit des services suivant : TikTok, Facebook, Instagram, LinkedIn, Whatsapp, Messenger, Google Maps, Play, Shopping et Search, Amazon et Meta Marketplace, App Store, Youtube, Chrome, Safari, Google Android, iOS, Windows PC OS, etc.
[801] CJUE, aff. T-1077/23.
[802] CJUE, aff. T-1080/23.
[803] CJUE, aff. T-1078/23.

279. Interdiction de collecter les données à caractère personnel de services tiers. Tout d'abord, il est désormais interdit de traiter les données à caractère personnel des utilisateurs qui recourent à des services de tiers utilisant les services de plateforme essentiels fournis par le contrôleur d'accès[804]. Autrement dit, il ne s'agit pas des données à caractère personnel directement transmises par l'utilisateur ou collectées mais les données provenant de services de tiers, c'est-à-dire de « sources extérieures[805] ». Les contrôleurs d'accès ne pourront donc plus récupérer les données issues d'interfaces intégrées ou de *cookies*. Il est d'usage pour ces plateformes de collecter les données de sites tiers à chaque fois que les utilisateurs se connectent sur leur site. Dès lors, la plateforme combine ces données « de l'extérieur » avec les données que la plateforme possède déjà sur l'utilisateur. De surcroît, il est désormais interdit de combiner les données à caractère personnel provenant du service de plateforme essentiel avec d'autres données à caractère personnel provenant de tout autre service de plateforme ou service fourni par le contrôleur d'accès[806]. Enfin, l'article 5 retient une logique similaire en interdisant le croisement des données à caractère personnel[807].

La logique d'interdiction de combinaison et de croisement des données à caractère personnel permet de ralentir le pouvoir de marché des géants du numérique sur la détention de données. En étant contrôleur d'accès, ils s'étaient permis de collecter et de croiser les données issues de leurs services et de services tiers. Leur position monopolistique leur permettait d'être en position de force avec les entreprises tierces qui n'avaient pas le choix d'être sur leur plateforme pour la visibilité. Pour les GAFAM, il s'agissait d'une autre source lucrative de données. Ainsi, par-delà leur collecte déjà massive de données à caractère personnel des utilisateurs, ils se servaient également des données collectées « de l'extérieur ».

280. Interdiction d'utilisation en concurrence des données commerciales. Le règlement invoque également les données commerciales : l'article 6.2 prévoit que le contrôleur d'accès n'utilise pas « en concurrence avec les entreprises utilisatrices, les données, quelles qu'elles soient, qui ne sont pas accessibles au public, qui sont générées ou fournies par ces entreprises

[804] Règlement (UE) 2022/1925 du Parlement européen et du Conseil du 14 septembre 2022 relatif aux marchés contestables et équitables dans le secteur numérique (règlement sur les marchés numériques), article 5 a).
[805] Roda Christophe, « Le Digital Markets Act (2e partie). Contraindre les contrôleurs d'accès », Communication commerce électronique, n° 3, Mars 2023.
[806] Règlement précité, article 5 b).
[807] *Ibid.*, article 5 c).

utilisatrices dans le cadre de leur utilisation des services de plateformes concernés, ou à l'appui de ceux-ci, y compris les données générées ou fournies par les clients de ces entreprises utilisatrices ». Dans cet article, sont visées les pratiques consistant à utiliser les données commerciales afin de promouvoir leurs propres produits à défaut des concurrents. En pratique, les contrôleurs d'accès ajustent leur offre en fonction des données captées auprès de vendeurs présents sur leur plateforme[808]. Les interdictions précitées permettent de renforcer la protection des utilisateurs.

II. Une réglementation renforcée favorable aux utilisateurs

281. Transparence et portabilité. En parallèle du règlement sur les marchés numérique, l'entrée en vigueur du Règlement (UE) 2022/2065 du 19 octobre 2022 du Parlement européen et du Conseil relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (règlement sur les services numériques) intensifie l'obligation de transparence pour les plateformes dominantes afin de les responsabiliser aux nouveaux risques du numérique (A). Par ailleurs, les nouveaux règlements précités renforcent la portabilité des données pour les utilisateurs dans le dessein de consolider leur contrôle sur les données (B).

A) Le renforcement insuffisant de l'obligation de transparence pour les plateformes dominantes

282. Plateformes dominantes. Toujours dans le dessein d'établir une régulation ciblée, le règlement sur les services numériques adapte son champ d'application aux plateformes dominantes. Autrement dit, à l'instar du règlement sur les marchés numériques, le règlement sur les services numérique cible les géants du numérique (1). Une fois qualifiées de dominante, les plateformes doivent respecter certaines obligations de transparence afin de protéger les individus contre certains risques inhérents à leurs pratiques (2).

[808] Douville Thibault, « Règlement sur les marchés numériques (digital markets act) : questions choisies sur son champ d'application après la désignation des premiers contrôleurs d'accès », RTD Com., 2023, p. 873.

1. L'adaptation nécessaire des catégories de plateformes aux géants du numérique

283. Reprise des anciennes distinctions. Fondé sur l'article 114 du Traité sur le fonctionnement de l'Union européenne, le règlement sur les services numériques a pour objectif de contribuer au bon fonctionnement du marché intérieur des services intermédiaires en établissant des règles harmonisées pour les services numériques, en particulier les plateformes[809]. Pour ce faire, le règlement reprend pour l'essentiel les anciennes distinctions selon la nature de l'activité : le service de « simple transport » consistant à transmettre, sur un réseau de communication, des informations fournies par un destinataire du service ou à fournir l'accès à un réseau de communication ; un service de « mise en cache » consistant à transmettre sur un réseau de communication des informations fournies par un destinataire du service, impliquant le stockage automatique, intermédiaire et temporaire de ces informations, effectué dans le seul but de rendre plus efficace la transmission ultérieure de ces informations à d'autres destinataires à leur demande ou encore un service d'«hébergement » consistant à stocker des informations fournies par un destinataire du service à sa demande[810]. Néanmoins, certaines qualifications étaient devenues obsolètes au regard des nouvelles pratiques.

284. Adaptation de la qualification d'hébergeur. La qualification d'hébergeur est devenue de plus en plus imprécise au regard du développement des nouveaux services : la qualification ne reflète plus la réalité en raison de l'utilisation des algorithmes de recommandation permettant aux plateformes d'avoir une incidence sur les contenus. Aujourd'hui, l'activité d'hébergeur peut revêtir diverses activités comme un forum, les réseaux sociaux, des *marketplaces* ou encore des services de *streaming*[811]. Afin de prendre en compte les diverses activités, le règlement ajoute une qualification spéciale au sein de la catégorie des hébergeurs : les plateformes et les moteurs de recherche. Selon l'article 3.i du règlement sur les services numériques, la plateforme en ligne est un service d'hébergement qui, à la demande d'un destinataire du service, stocke et diffuse au public des informations, à moins que cette activité ne soit une caractéristique mineure et purement accessoire d'un autre service ou une fonctionnalité mineure du service principal. Par exemple, les réseaux sociaux et les places de marché entrent dans cette nouvelle catégorie.

[809] Règlement (UE) 2022/2065 du 19 octobre 2022 du Parlement européen et du Conseil relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (règlement sur les services numériques), article 1, point 1.
[810] *Ibid.*, article 2 paragraphe 1.
[811] Merabet Samir, « Le Digital Service Act : permanence des acteurs, renouvellement des qualifications », La Semaine Juridique édition générale n° 41, 17 octobre 2022, 1175.

Concernant les moteurs de recherche, il s'agit d'un service intermédiaire qui permet aux utilisateurs de formuler des requêtes[812]. Les nouvelles catégories sont considérées comme des « sous-catégories » de plateformes en ligne[813].

285. Création de la catégorie des « très grandes plateformes ». Au-delà d'intégrer de nouvelles sous-catégories, la simple distinction selon la nature de l'activité était devenue anachronique et injuste. L'unique régime s'appliquait de manière uniforme entre un site amateur ou un réseau social aux millions d'utilisateurs[814]. Ainsi, le règlement instaure une distinction selon le volume de l'activité : les très grandes plateformes et les très grands moteurs de recherche en ligne vont se voir imposer des exigences supplémentaires compte tenu de leur portée et de leur rôle particuliers[815]. Le seuil quantitatif imposé à l'article 33 est celui du « nombre mensuel moyen de destinataires actifs du service dans l'Union égal ou supérieur à 45 millions »[816]. L'ajout d'un seuil quantitatif et d'une nouvelle catégorie permet de cibler spécifiquement les géants du numérique et de ne pas pénaliser les petites et moyennes entreprises. L'instauration d'un règlement avec des obligations graduées en fonction de la taille de la société était nécessaire.

286. Désignation des « très grandes plateformes ». Plusieurs plateformes vont être désignées dans un premier temps par la Commission européenne : AliExpress, Amazon Store, Apple, AppStore, Bing, Booking, Facebook, Google Maps, Google Play, Google Search, Google Shopping, Instagram, LinkedIn, Pinterest, Snapchat, TikTok, Wikipedia, X (anciennement Twitter), YouTube et Zalando[817]. Toutes ces entreprises avaient jusqu'au 25 août 2023 pour se conformer aux obligations du règlement précité. Le 20 décembre 2023, la Commission a désigné trois sites pornographiques de « très grandes plateformes » (Pornhub, Stripchat et XVideos)[818]. Plus récemment, le 26 avril 2024, la plateforme Shein a également été

[812] Règlement (UE) 2022/2065 du 19 octobre 2022 du Parlement européen et du Conseil relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (règlement sur les services numériques), article 3 point j).
[813] *Ibid.*, considérant 13.
[814] Merabet Samir, *op. cit*.
[815] Règlement (UE) 2022/2065 du 19 octobre 2022 du Parlement européen et du Conseil relatif à un marché unique des services numériques, considérant 48.
[816] *Ibid.*, article 33.
[817] Commission européenne, « Services numériques : La Commission désigne le premier ensemble de très grandes plateformes en ligne et de moteurs de recherche », Communiqué de presse, 25 avril 2023.
[818] Commission européenne, « La Commission désigne une deuxième série de très grandes plateformes en ligne au titre du règlement sur les services numériques », Communiqué de presse, 20 décembre 2023.

désignée[819]. À l'instar du règlement sur les marchés numériques, plusieurs plateformes ont contesté leurs désignations, tel est le cas des plateformes Zalando[820] et Amazon[821].

Ainsi, en fonction de leurs nouvelles qualifications, de nouvelles obligations sont instaurées par le règlement sur les services numériques. Les obligations sont désormais proportionnelles selon la taille et le rôle des plateformes. En réalité, certaines obligations nous paraissent encore insuffisantes.

2. L'adaptation insuffisante des mesures aux risques en ligne

287. Transparence et signaleur de confiance. Tout d'abord, certaines obligations concernent la lutte contre les contenus illicites. À cet égard, les plateformes doivent proposer un outil aux utilisateurs leur permettant de signaler facilement ces contenus. Une fois le signalement effectué, les plateformes ont l'obligation de réagir rapidement tout en respectant les droits fondamentaux. Pour cela, elles doivent coopérer avec des signaleurs de confiance. L'instauration de ces nouveaux acteurs permet d'introduire des acteurs légitimes dans la modération des contenus. En effet, les signaleurs de confiance sont des entités désignées par les coordinateurs nationaux pour les services numériques. L'attribution de ce statut s'effectue selon des critères spécifiques tels que l'objectivité et l'indépendance[822]. Spécifiquement, le critère d'indépendance est primordial afin d'effectuer une modération légitime. L'auto-modération effectuée par les plateformes est dangereuse : les géants du numérique sont motivés par des intérêts mercantiles, rendant leur modération privée et opaque. À titre d'illustration, les plateformes pratiquent le « *shadow banning* » sur les réseaux sociaux : il s'agit d'une pratique

[819] Commission européenne, « La Commission désigne Shein en tant que très grande plateforme en ligne, au titre du règlement sur les services numériques », Communiqué de presse, 28 avril 2024.
[820] CJUE, aff. T-348/23.
[821] CJUE, aff. T-367/23.
[822] Règlement (UE) 2022/2065 du 19 octobre 2022 du Parlement européen et du Conseil relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (règlement sur les services numériques), article 22, point 2 : « Le statut de signaleur de confiance au titre du présent règlement est attribué, sur demande présentée par une entité, quelle qu'elle soit, par le coordinateur pour les services numériques de l'État membre dans lequel l'entité présentant la demande est établie, à l'entité présentant la demande qui a démontré qu'elle remplit l'ensemble des conditions suivantes: a) elle dispose d'une expertise et de compétences particulières aux fins de détecter, d'identifier et de notifier des contenus illicites; b) elle est indépendante de tout fournisseur de plateformes en ligne; c) elle exerce ses activités aux fins de la soumission des notifications de manière diligente, précise et objective. ».

opaque par laquelle les plateformes diminuent la visibilité d'un utilisateur à son insu[823]. Les plateformes freinent alors la diffusion de contenus non souhaitables, sans réellement prendre de mesure contre l'utilisation en question. La censure est alors entièrement opaque et silencieuse. Désormais, l'article 14 du règlement sur les services numériques oblige les plateformes à améliorer leur transparence en exposant dans leurs conditions générales leurs règles de modération, dans un langage clair et univoque[824]. En somme, les plateformes vont devoir rendre des comptes sur leurs techniques inintelligibles utilisées jusqu'à présent.

288. Interdiction des interfaces trompeuses. Toujours dans le dessein de renforcer la transparence, les interfaces trompeuses sont désormais prohibées. Pour la première fois en Europe, les interfaces trompeuses sont expressément interdites par un texte contraignant[825]. Le considérant 67 du règlement sur les services numériques précise qu'il devrait être interdit pour les plateformes « de tromper ou d'encourager dans un sens les destinataires du service et d'altérer ou d'entraver l'autonomie, la prise de décision ou le choix des destinataires du service par la structure, la conception ou les fonctionnalités d'une interface en ligne ou d'une partie de celle-ci[826] ». Ainsi, les interfaces en ligne destinées à tromper ou à manipuler les utilisateurs sont interdites. Néanmoins, au regard des pratiques opaques de ces acteurs, il conviendra d'étudier l'effectivité de ces mesures[827].

---

[823] Chatelain Yannick, « La censure par invisibilisation des "démocraties" ? Le phénomène du "Shadow Banning" », Forbes, 2 avril 2024 : « Le "Shadow Banning", également connu sous le nom de "stealth banning", "ghost banning" ou encore "comment ghosting", ce qui peut être traduit en français par "bannissement furtif" ou "bannissement silencieux" est une pratique extrêmement controversée sur les réseaux sociaux. ».

[824] Règlement (UE) 2022/2065 du 19 octobre 2022 du Parlement européen et du Conseil relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (règlement sur les services numériques), article 14, point 1 : « Les fournisseurs de services intermédiaires incluent dans leurs conditions générales des renseignements relatifs aux éventuelles restrictions qu'ils imposent en ce qui concerne l'utilisation de leur service vis-à-vis des informations fournies par les destinataires du service. Ces renseignements comprennent des informations sur les politiques, procédures, mesures et outils utilisés à des fins de modération des contenus, y compris la prise de décision fondée sur des algorithmes et le réexamen par un être humain, ainsi que sur le règlement intérieur de leur système interne de traitement des réclamations. Ils sont énoncés dans un langage clair, simple, intelligible, aisément abordable et dépourvu d'ambiguïté, et sont mis à la disposition du public dans un format facilement accessible et lisible par une machine. ».

[825] Potel-Saville Marie, « Dark Patterns : l'étau législatif se resserre (enfin ?) sur les interfaces manipulatrices ou trompeuses », RPPI, LexisNexis, 2022, dossier 19.

[826] Règlement (UE) 2022/2065 du 19 octobre 2022 du Parlement européen et du Conseil relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (règlement sur les services numériques), considérant 67.

[827] *Infra*., Titre 2 sur l'effectivité des normes.

289. Protection des mineurs. Par ailleurs, la publicité ciblée pour les mineurs est interdite. La protection des mineurs est l'un des objectifs du règlement sur les services numériques. Les plateformes ne pourront plus présenter de publicité qui repose sur le profilage utilisant des données à caractère personnel lorsqu'ils savent qu'il s'agit d'un mineur[828]. La proposition paraît conforme au bon sens pourtant, les mineurs constituent des cibles pour les plateformes. En application du principe de minimisation du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, les plateformes ne doivent pas recueillir davantage de données afin d'évaluer si le destinataire du service est un mineur. Dans l'hypothèse où les fournisseurs de services intermédiaires s'adressent principalement aux mineurs ou lorsque le service est utilisé de manière prédominante par ces derniers, les fournisseurs doivent déployer des « efforts particuliers » pour rendre la compréhension de leurs conditions générales aisée pour les mineurs. En pratique, les conditions générales sont déjà généralement inintelligibles pour les personnes majeures, il est donc possible de douter de l'efficacité de cette mesure[829].

290. Opacité des mesures internes. En réalité, le règlement sur les services numériques n'est pas assez sévère en matière de responsabilité des plateformes : le règlement responsabilise les acteurs dans un esprit de *compliance*. Il est attendu que les plateformes participent à la régulation de leurs plateformes, sans assumer directement la responsabilité de leurs conséquences dommageables. L'inintelligibilité de leurs pratiques permet à ces acteurs d'avoir le rôle principal dans la construction du cadre les incombant[830]. Par ailleurs, le règlement met en place un système de régulation impliquant un dialogue entre les régulateurs et les plateformes[831]. L'article 34 du règlement sur les services numériques prévoit que les

[828] Règlement (UE) 2022/2065 du 19 octobre 2022 du Parlement européen et du Conseil relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (règlement sur les services numériques), considérant 71.

[829] *Infra.*, n° 501.

[830] Loiseau Grégoire « Le Digital Services Act », CCE, n°2, février 2023, étude 3 : « Dans cette construction, les plateformes ont le rôle principal. C'est à elles qu'il incombe, dans le cadre juridique auquel elles doivent se conformer, de concevoir et d'activer les dispositifs afin de procéder au traitement des contenus illicites et d'œuvrer à la résorption de certains risques, le cas échéant systémiques, liés à leur fonctionnement. ».

[831] G'Sell Florence, « Les réseaux sociaux ou la privatisation de l'espace informationnel en ligne », RDIA, n°5, mai 2022, p. 57 : « C'est ainsi que le DSA permet de demander des comptes aux plateformes sur des points essentiels qui restaient jusqu'à présent à la seule main des dirigeants de ces entreprises : la manière dont les architectures et les algorithmes, à commencer par les systèmes de recommandation, sont conçus, les stratégie publicitaire mise en œuvre par la plateforme (article 34.2) etc. Il reste, cependant, possible de douter

plateformes doivent évaluer leurs « risques systémiques » afin de prendre les mesures appropriées pour les réduire[832]. Il est toutefois légitime de douter de l'efficacité de mesures internes de la part de sociétés privées. Grâce à la maîtrise de leur environnement, les plateformes déterminent les mesures à mettre en place : les plateformes réduisent les risques sans pour autant éradiquer l'ensemble des contenus illicites, contenus indispensables pour leur modèle d'affaires. Tant que les plateformes choisiront les mesures à mettre en place, les mesures de modération resteront insuffisantes. Les géants du numérique sont des sociétés privées et prennent leurs décisions dans une logique économique et non altruiste.

Par-delà les obligations instaurées pour les plateformes, les règlements sur les services et marchés numériques se mobilisent pour renforcer le contrôle des individus sur leurs données par le droit à la portabilité.

B) L'importance du renforcement de la portabilité des données pour les utilisateurs

291. Portabilité « effective » et « renforcée ». Afin de prolonger le contrôle des individus sur leurs données instauré par le Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, le DMA consacre une portabilité « effective » des données fournies ou générées (1). En parallèle, le Règlement (UE) 2023/2854 du Parlement européen et du Conseil du 13 décembre 2023 concernant des règles harmonisées portant sur l'équité de l'accès aux données et de l'utilisation des données crée une portabilité « renforcée » sur les données générées par les objets connectés (2).

de l'efficacité du dialogue instauré avec les régulateurs par la remise de rapports réguliers et la faculté pour ceuxci d'émettre des lignes directrices. ».

[832] Règlement (UE) 2022/2065 du 19 octobre 2022 du Parlement européen et du Conseil relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (règlement sur les services numériques), article 34 « Évaluation des risques » : « Les fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne recensent, analysent et évaluent de manière diligente tout risque systémique au sein de l'Union découlant de la conception ou du fonctionnement de leurs services et de leurs systèmes connexes, y compris des systèmes algorithmiques, ou de l'utilisation faite de leurs services. ».

1. La consécration d'une portabilité effective des données fournies ou générées

292. Droit à la portabilité « effective » : principe. L'article 6.9 du Règlement (UE) 2022/1925 du Parlement européen et du Conseil du 14 septembre 2022 relatif aux marchés contestables et équitables dans le secteur numérique prévoit que « le contrôleur d'accès assure aux utilisateurs finaux et aux tiers autorisés par un utilisateur final, à leur demande et gratuitement, la portabilité effective des données fournies par l'utilisateur final ou générées par l'activité de l'utilisateur final dans le cadre de l'utilisation du service de plateforme essentiel concerné, y compris en fournissant gratuitement des outils facilitant l'exercice effectif de cette portabilité des données, et notamment en octroyant un accès continu et en temps réel à ces données ». Le droit à la portabilité complète celui énoncé dans le Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016. Il a cependant un champ d'application plus large puisqu'il concerne non plus exclusivement les données à caractère personnel mais également les également les données d'interaction[833], données fournies par l'utilisateur final ou générées par l'activité dans le cadre de l'utilisation de service[834].

293. Droit à la portabilité « effective » : conditions techniques. Afin que la portabilité soit réellement « effective », le règlement prévoit que les contrôleurs d'accès garantissent la portabilité « y compris en fournissant gratuitement des outils facilitant l'exercice effectif de cette portabilité des données, et notamment en octroyant un accès continu et en temps réel à ces données[835]». Au demeurant, les données doivent être transmises dans un format structuré, couramment utilisé et lisible par machine[836] : la portabilité et l'interopérabilité des données doivent être facilitées par l'utilisation de normes techniques[837]. Pour les contrôleurs d'accès, l'application du droit à la portabilité pourra constituer une charge financière et technique au regard du nombre de données à caractère personnel et de données à caractère non personnel traitées par ces acteurs. Pour autant, cette obligation ne concerne que les acteurs qualifiés de contrôleurs d'accès. Dès lors qu'ils disposent des moyens de traiter ces données, ils doivent

---

833 Zolynski Célia, « Liberté de circulation et personne concernée : les apports du droit à la portabilité », *in* Bruguière Jean-Michel, *L'émergence d'un droit des données*, éd. Dalloz, 2023, p. 144.

834 Règlement (UE) 2022/1925 du Parlement européen et du Conseil du 14 septembre 2022 relatif aux marchés contestables et équitables dans le secteur numérique, considérant 9.

835 *Ibid.*

836 Règlement (UE) 2022/1925 du Parlement européen et du Conseil du 14 septembre 2022 relatif aux marchés contestables et équitables dans le secteur numérique, considérant 59.

837 *Ibid.*, considérant 96.

avoir - ou développer - les moyens de faire respecter les droits des utilisateurs. Le renforcement du droit à la portabilité est important pour les utilisateurs. Ils peuvent reprendre le contrôle de leurs données et changer de services facilement. Toutefois, il est important de partager la connaissance de ce droit aux utilisateurs pour qu'il puisse être effectif.

À l'instar du droit à la portabilité effective, le Règlement (UE) 2023/2854 du Parlement européen et du Conseil du 13 décembre 2023 concernant des règles harmonisées portant sur l'équité de l'accès aux données et de l'utilisation des données (règlement sur les données) créé une portabilité renforcée pour les données générées par des objets connectés.

2. La création d'une portabilité renforcée des données générées par les objets connectés

294. Droit à la portabilité « renforcé » pour les utilisateurs et les professionnels. Les objets connectés génèrent des données d'utilisation du produit ou du service. En pratique, le fabricant ou le concepteur d'un produit détient généralement un contrôle exclusif sur ces données. De ce fait, les données générées par des produits ou services liés ne sont pas aisément accessibles à leurs utilisateurs et les possibilités de portabilité sont limitées[838]. Le Règlement (UE) 2023/2854 du Parlement européen et du Conseil du 13 décembre 2023 concernant des règles harmonisées portant sur l'équité de l'accès aux données et de l'utilisation des données (règlement sur les données) étend la portée du droit à la portabilité pour les utilisateurs afin de contrôler l'utilisation de leurs données générées par l'utilisation de l'Internet des objets en imposant une portabilité renforcée de leurs données à caractère personnel et données à caractère non personnel aux fournisseurs d'objets connectés[839]. Par ailleurs, la portabilité de ces données renforce l'offre concurrentielle de services après-vente et permet de développer l'innovation sur les données. En outre, ce renforcement prolonge la « durée de vie » des produits connectés, dans l'intérêt de la protection de l'environnement et par conséquent, du respect du « Pacte vert »[840].

---

[838] Règlement (UE) 2023/2854 du Parlement européen et du Conseil du 13 décembre 2023 concernant des règles harmonisées portant sur l'équité de l'accès aux données et de l'utilisation des données (règlement sur les données), considérant19.

[839] Zolynski Célia, *op. cit*.

[840] Commission européenne, « Le pacte vert pour l'Europe », Communication de la Commission au Parlement européen, au Conseil européen, au Conseil, au Comité économique et social européen et au Comité des régions, COM(2019) 640 final.

295. Droit à la portabilité « objectif ». De la même manière que le Règlement (UE) 2022/1925 du Parlement européen et du Conseil du 14 septembre 2022 relatif aux marchés contestables et équitables dans le secteur numérique, ledit règlement prévoit un champ plus large pour la nature des données : il s'agit de toutes les données générées par l'utilisation d'un produit ou d'un service, « quelle que soit la nature en tant que données à caractère personnel, sans distinction entre les données activement fournies et les données observées passivement »[841]. Ainsi, il s'agit d'un droit à la portabilité « objectif », sans distinction de la nature des données. Pour rendre effectif ce droit à la portabilité, le règlement énonce une obligation de rendre accessibles les données générées pour les fournisseurs (article 3), un droit d'accès à ces données pour les utilisateurs (article 4) et la faculté de partager ces données avec des tiers (article 5). Les utilisateurs peuvent faire usage du droit à la portabilité afin de reprendre le contrôle sur leurs données. En pratique, les géants du numérique ne doivent pas rendre la mise en œuvre de ce droit complexe. Le droit à la portabilité n'étant pas dans l'intérêt économique de ces acteurs, il conviendra de surveiller les pratiques des plateformes à ce sujet.

[841]Règlement (UE) 2023/2854 du Parlement européen et du Conseil du 13 décembre 2023 concernant des règles harmonisées portant sur l'équité de l'accès aux données et de l'utilisation des données (règlement sur les données), considérant 31.

296. Conclusion de la section. La consolidation du marché unique numérique nécessite une réglementation concurrentielle des données. En effet, la position monopolistique des géants du numérique impacte l'accès et la circulation des données. La collecte massive de données ainsi que la combinaison de ces données a permis à certains acteurs du numérique de détenir un pouvoir de marché démesuré. L'accumulation de ces données leur permet de renforcer leur position de force et d'éviter l'intégration de nouveaux acteurs. Or, le droit de la concurrence a spécifiquement pour dessein de maintenir une concurrence libre et non faussée.

Néanmoins, le fonctionnement disruptif des géants du numérique a mis en exergue l'inadaptation du droit de la concurrence à sanctionner leurs positions dominantes. Le droit de la concurrence nécessite des preuves impossibles à rapporter au regard des pratiques opaques des géants du numérique. De surcroît, le temps considérable des enquêtes n'est pas adapté à la célérité de leurs pratiques. Ainsi, l'Union européenne s'est heureusement saisie de cette problématique en élaborant une réglementation ciblée et concurrentielle des données.

Les nouveaux règlements 2022/1925 du 14 septembre 2022 relatif aux marchés contestables et équitables dans le secteur numérique et 2022/2065 du 19 octobre 2022 du Parlement européen et du Conseil relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE ciblent directement les grands acteurs du numérique et leurs pratiques sur la détention massive de données. Les principales mesures sont l'interdiction de combiner et croiser des données à caractère personnel des utilisateurs, afin de lutter contre l'accumulation massive des données. De plus, le règlement sur les services numériques renforce les obligations de transparence des plateformes.

Néanmoins, les récents règlements responsabilisent les acteurs du numérique dans une logique de *compliance*. Les géants du numérique deviennent les protagonistes de la construction normative sur les données. En réalité, il s'agit de sociétés privées agissant dans une logique lucrative. Les principales décisions de ces acteurs sont imprégnées d'une logique économique et non d'une logique altruiste. La logique de responsabilisation des acteurs sur leurs propres technologies est utopique. Par ailleurs, l'Union européenne souhaite désormais contraindre les géants du numérique à partager leurs données. Dans une stratégie holistique, l'Union européenne engage désormais une régulation globale afin de favoriser la circulation des données. En réalité, les géants du numérique profitent de l'ouverture des données, rendant chimérique l'objectif d'une réglementation globale.

Section 2 : L'objectif chimérique d'une réglementation globale pour l'ouverture des données

297. Régulation globale par la confiance. L'élaboration d'un marché unique des données nécessite une réglementation globale des données : la libéralisation des flux de données doit être élaborée dans un cadre de partage de confiance. Il s'agit désormais de prolonger la politique d'ouverture des données et l'ouverture concerne toutes les données, c'est-à-dire les données à caractère personnel et les données à caractère non personnel, comprenant les données publiques et les données industrielles liées à l'Internet des objets.

Ainsi, dans une logique antinomique aux géants du numérique, l'Union européenne entend élaborer un modèle disruptif de partage de données afin de libérer le flux de données et permettre le développement de l'intelligence artificielle (I). Néanmoins, l'ouverture excessive des données emporte inévitablement des conséquences défavorables pour les utilisateurs, conséquences qui s'avèrent favorables pour les géants du numérique (II).

I. L'élaboration d'un modèle disruptif de partage des données

298. Création de modèle alternatif. Contrairement au modèle des géants du numérique - c'est-à-dire l'accumulation massive et fermée des données - l'Union européenne souhaite établir un modèle alternatif de partage de données. Pour ce faire, le Règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données (règlement sur la gouvernance des données) favorise la disponibilité des données en renforçant les mécanismes de partage de données dans un cadre de confiance. L'élaboration de ce cadre nécessite la mise en place d'une gouvernance de confiance (A), grâce à la création d'un écosystème de confiance (B).

A) La mise en place d'une gouvernance de confiance

299. Partage des données. Afin de favoriser le partage des données, l'Union européenne a élaboré deux textes majeurs : le règlement sur la gouvernance des données et le règlement sur les données[842]. Il s'agit de renforcer l'ouverture de données à caractère non personnel ayant un intérêt stratégique et économique important : les données publiques et les données industrielles. Ainsi, d'une part, le règlement sur la gouvernance des données prolonge et renouvelle la politique d'ouverture des données publiques (1) et d'autre part, le règlement sur les données permet la mise à disposition des données industrielles (2).

1. Le renouvellement de la politique d'ouverture des données publiques

300. Entrée en vigueur du Règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données (DGA). Le règlement sur la gouvernance européenne des données est entré en vigueur le 23 juin 2022 et sera applicable à partir du 24 septembre 2023, sans préjudice des règlements sectoriels préexistants, notamment en matière de protection des données à caractère personnel. Le règlement européen sur la gouvernance des données vise à favoriser la disponibilité des données en renforçant les mécanismes de partage de données dans l'ensemble de l'Union européenne. En effet, le règlement a été élaboré à la suite d'une analyse d'impact relevant le manque de confiance et les difficultés techniques pour le partage des données publiques[843]. La politique d'*open data* instaurée par la Directive 2019/1024 ayant été insuffisamment mise en œuvre, l'Union européenne a repris le mouvement d'ouverture pour valoriser les données publiques.

301. Limites de la politique d'*open data* : les données protégées. Tout d'abord, le règlement sur la gouvernance des données réaffirme la valeur des données publiques, représentant des enjeux économiques importants[844]. La politique d'*open data* menée jusque-là a été limitée par la protection de certaines données, comme certaines catégories de données protégées par des droits d'autrui : il peut s'agir de données protégées par la confidentialité commerciale ou les

[842] Martial-Braz Nathalie. « Deux Acts pour une stratégie numérique ! », CCE, n° 9, septembre 2023.
[843] Commission européenne, « Impact assessment report accompanying the DGA proposal », Rapport, SWD(2020), 295 final, p. 5.
[844] Mouncif-Moungache Mouna, « Le règlement sur la gouvernance des données ou l'émergence d'un modèle européen », *in* Eynard Jessica et Castets-Renard Céline (dir.), *Un droit de l'intelligence artificielle. Entre règles sectorielles et régime général. Perspectives comparées*, éd. Bruylant, 2023, p. 506.

droits de propriété intellectuelle ou par les droits à la protection des données à caractère personnel. De fait, l'ouverture de ces données est soumise à des exigences procédurales de nature technique et juridique conduisant à une sous-utilisation de ces données[845].

302. Renouvellement de la politique d'ouverture des données publiques. Ainsi, le règlement sur la gouvernance des données étend la politique d'ouverture des données publiques aux données protégées[846]. Il est précisé que le règlement « complète » la Directive (UE) 2019/1024 du Parlement européen et du Conseil du 20 juin 2019 concernant les données ouvertes et la réutilisation des informations du secteur public[847] : le champ d'application de l'ouverture des données publiques est élargi aux données protégées. En revanche, les données protégées pour des raisons de sécurité publique, de sécurité nationale ou de défense sont exclues. Néanmoins, le règlement n'impose pas l'ouverture de ces données[848] : il s'agit d'établir un cadre pour les organismes du secteur public souhaitant ouvrir ces données.

In fine, le règlement prolonge le mouvement « simplement » incitatif d'ouverture des données publiques. Pourtant, les données protégées ne sont pas la principale cause du relâchement de la politique d'ouverture des données publiques. Tant que les administrations ne disposeront pas des moyens techniques et des formations nécessaires, les données ouvertes - qu'importe leur nature - ne seront pas réellement réutilisables. Par ailleurs, le règlement sur les données instaure l'ouverture d'un nouveau type de données : les données industrielles.

---

845 Règlement (UE) 2022/868 du 30 mai 2022 portant sur la gouvernance européenne des données, considérant 5.

846 Hulin Anne-Sophie, « La gouvernance des données de l'IA ou l'avènement d'une nouvelle ère normative en droit du numérique", *in* Eynard Jessica et Castets-Renard Céline (dir.), *op. cit*.

847 Règlement (UE) 2022/868 du 30 mai 2022 portant sur la gouvernance européenne des données, exposé des motifs, p. 1.

848 Perray Romain et Favreau Julie, « Data Governance Act : le cerbère de la réutilisation des données ? », CCE, n° 3, Mars 2023.

2. La récente mise à disposition des données industrielles

303. Importance des données industrielles. Il existe une grande partie de données industrielles à caractère non personnel générées par des machines. Le développement des objets connectés dans notre vie quotidienne augmente cette masse de données[849] et la majorité de ces données est concentrée entre les mains de grandes entreprises, notamment par les géants du numérique. En effet, ils sont les principales entreprises à commercialiser leurs propres objets connectés. L'expansion des objets connectés étant encore en cours de développement, l'Union européenne souhaite dès à présent ouvrir l'accès à ces données avant l'agrégation monopolistique de certains acteurs du numérique.

304. Entrée en vigueur du Règlement du Parlement et du Conseil fixant des règles harmonisées pour l'équité de l'accès aux données et de l'utilisation des données (règlement sur les données). Ainsi, le règlement sur les données a été adopté par la Commission le 23 février 2022. Il s'agit d'un texte horizontal établissant un socle commun qui s'ajoute aux législations sectorielles préexistantes[850]. Les données concernées sont très hétéroclites puisqu'il s'agit des données industrielles, à caractère non personnel ou personnel, dont les métadonnées relatives au produit connecté ou au service[851]. Outre les données fournies par les individus, le règlement inclut les données résultant de l'observation tant du comportement actif que passif de la personne concernée[852]. Le règlement impose le partage afin que les micros, petites et moyennes entreprises, puissent récupérer des données afin d'en extraire de la valeur et l'améliorer l'innovation. Cette fois-ci, l'objectif est louable car il prend en compte les petites et moyennes entreprises dans la politique d'ouverture des données.

---

[849] Bergé Jean-Sylvestre et Le Métayer Daniel, « Phénomènes de masse et droit des données », Communication commerce électronique, 2018 ; Debet Anne « Quand les jouets nous espionnent », Communication, commerce électronique, 2018.

[850] Idot Laurence, « DMA, DSA, DGA, DA ou les dernières avancées du marché des services numériques », Europe n° 8-9, Août-septembre 2022.

[851] Proposition de règlement relatif à des règles harmonisées sur un accès équitable aux données et sur leur utilisation (règlement sur les données), COM(2022) 68 final, article 5 (2) : « Lorsqu'un utilisateur ou une partie agissant au nom de ce dernier en fait la demande, le détenteur de données met à la disposition d'un tiers, dans les meilleurs délais, sans frais pour l'utilisateur et, le cas échéant, en continu et en temps réel, les données générées par l'utilisation d'un produit ou d'un service lié, à un niveau de qualité identique à celui dont lui-même bénéficie. ».

[852] Perray Romain, « Data Act : une loi pour mieux distribuer la manne des données », LexisNexis, Revue trimestrielle, 2024.

305. Accessibilité et partage de données. Conformément à l'objectif du règlement, les premières mesures sont relatives au partage de données entre entreprises et consommateurs et interentreprises (chapitre II). Le règlement pose un principe d'accessibilité directe des données générées par les produits ou services : l'utilisateur aura le droit d'accéder, d'utiliser et de partager ces données avec des tiers[853]. Le droit d'accès pour l'utilisateur concerne les « données générées par l'utilisation du produit » et non seulement les données brutes insérées par l'utilisateur[854]. Le principe d'accessibilité directe renforce la sécurité juridique pour les consommateurs et les entreprises. En effet, le partage des données avec des tiers permet de remédier aux effets de verrouillage et d'entrave des services après-vente. Les consommateurs auront donc un choix plus large de services après-vente puisque les réparations ne pourront plus être réalisées exclusivement par le fabricant. Les petites et moyennes entreprises seront exemptées de ces obligations, l'objectif étant surtout de contraindre les acteurs en position de force sur le marché des données.

306. Interdiction des clauses abusives. Par ailleurs, afin de réduire certaines pratiques anticoncurrentielles, la proposition de règlement instaure un système de protection contre les clauses contractuelles abusives dans le cadre du partage des données (chapitre IV). En pratique, la détention monopolistique des données par les géants du numérique leur permet d'insérer des clauses contractuelles abusives. Ainsi, le règlement adapte le droit des contrats pour empêcher les parties fortes de tirer parti abusivement des déséquilibres en matière de négociation au détriment des parties les plus faibles. Dès lors, la liberté contractuelle est limitée en matière d'accès d'utilisation des données lorsque les clauses imposées unilatéralement sont qualifiées d'abusives[855] .

Pour garantir l'équité et de favoriser l'accès à ces données à des acteurs de bonne foi, le règlement précise que les entreprises désignées de contrôleur d'accès sont exclues du droit d'accès à ces données[856]. Dans ce règlement, l'Union européenne prend acte des faiblesses des

[853] Les contrôleurs d'accès au sens du DMA sont exclus du champ des « tiers ».

[854] Keller Jonathan, « Le Data Act : de nouvelles règles de partage des données », Dalloz Actualité, 20 décembre 2023.

[855] Règlement du Parlement et du Conseil fixant des règles harmonisées pour l'équité de l'accès aux données et de l'utilisation des données, article 13, point 2 : La clause abusive est définie comme une clause « d'une nature telle que son utilisation s'écarte fortement des bonnes pratiques commerciales en matière d'accès aux données et d'utilisation de celles-ci, et qu'elle est contraire à la bonne foi et à la loyauté. ».

[856] Règlement (UE) 2023/2854 du Parlement européen et du Conseil du 13 décembre 2023 concernant des règles harmonisées portant sur l'équité de l'accès aux données et de l'utilisation des données (règlement sur

derniers règlements afin d'écarter les géants du numérique et de favoriser les petites et moyennes entreprises. L'objectif économique de promotion des entreprises européennes est imprégné dans le règlement sur les données. Ainsi, un certain « écosystème de confiance » serait en train d'éclore afin de partager davantage de données.

B) La mise en place d'un écosystème de confiance

307. Notion de confiance. Dans un environnement où les géants du numérique ont profité de la confiance des utilisateurs pendant plusieurs années, il était nécessaire de rétablir - ou d'établir - un écosystème de confiance. Pour ce faire, le Règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données établit des garants de la confiance : les services intermédiaires de données (1). Une fois la confiance acquise pour le partage de données, la masse de données partagée va permettre le développement d'une intelligence artificielle de confiance (2).

1. Le développement d'un partage de confiance

308. Cadre de confiance collectif. Avec les récents scandales et la prise de conscience des utilisateurs sur l'exploitation de leurs données, le partage des données est inévitablement limité. En effet, les utilisateurs n'ouvrent pas leurs données par crainte de réutilisation abusive de leurs données à caractère personnel et du côté des entreprises, ces dernières sont également réticentes par crainte d'usages ultérieurs de leurs données au détriment de la concurrence[857]. Allant plus loin que le règlement sur la protection des données à caractère personnel établissant un cadre de confiance bilatérale (entre le responsable de traitement et la personne), les nouveaux règlements instaurent un cadre de confiance collectif, voire une confiance « systémique[858] » : il s'agit d'établir un cadre de confiance dans lequel les individus et les entreprises sont enclins à

---

les données), considérant 36 : « Conformément au [règlement sur les marchés contestables et équitables dans le secteur numérique], et compte tenu de la capacité sans égale de ces entreprises en matière d'acquisition de données, il ne serait pas nécessaire, pour atteindre l'objectif du présent règlement, et serait donc disproportionné à l'égard des détenteurs de données soumis à de telles obligations, d'inclure ces entreprises désignées contrôleur d'accès parmi les bénéficiaires du droit d'accès aux données. ».

[857] Commission nationale de l'informatique et des libertés, « Les enjeux économiques de la mise en œuvre du règlement sur la gouvernance des données », étude économique destinée aux professionnels, 2023, disponible en ligne.

[858] Hulin Anne-Sophie « La gouvernance des données de l'IA ou l'avènement d'une nouvelle ère normative en droit du numérique », *op. cit*., p. 485.

partager leurs données[859]. À ce sujet, la Commission nationale de l'informatique et des libertés a publié des recommandations sur le partage des données par des API dans un cadre de confiance[860].

309. Notion de confiance. La notion de confiance est un élément central du règlement sur la gouvernance des données. En effet, la notion de confiance est omniprésente dans le texte. Il s'agit de « renforcer la confiance[861] », « d'accroître la confiance[862] », de garantir un « niveau plus élevé de confiance[863] », d'instaurer la confiance dans le partage des données, ou encore en citant des « échanges de données digne de confiance »[864]. Le règlement précise que la gouvernance des données permet d'instaurer la confiance dans le partage des données et d'assurer le respect des droits fondamentaux tout au long du cycle de vie d'un jeu de données[865]. Autrement dit, la gouvernance serait constituée des « différents régimes ou protections juridiques existant sur une ou plusieurs données, tout au long de son cycle de vie, ainsi que les

[859] Poullet Yves, « 50 ans de législations européennes de protection des données. Hier, aujourd'hui et demain. », *in* Bévière-Boyer Bénédicte, Dibie Dorothée et Arlotti Clément (dir.), *Numérique, droit et société,* éd. Dalloz, 2022, p. 40.

[860] Commission nationale de l'informatique et des libertés, « Recommandation technique relative à l'utilisation des interfaces de programmation applicatives (API) pour le partage sécurité de données à caractère personnel », 24 novembre 2023.

[861] Règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données (règlement sur la gouvernance des données), p. 8 : « Le chapitre IV facilite l'altruisme des données (données mises volontairement à disposition par des particuliers ou des entreprises, pour le bien commun). Il prévoit la possibilité, pour les organisations qui pratiquent l'altruisme des données, de s'enregistrer en tant qu'"organisation altruiste en matière de données reconnue dans l'Union européenne" afin de renforcer la confiance dans leurs activités. » .

[862] *Ibid.,* p. 3 : « Le cadre de notification concernant les intermédiaires de données, ainsi que les mécanismes relatifs à l'altruisme en matière de données, permettent d'accroître la confiance dans ces services, sans restreindre inutilement ces activités, et contribuent au développement d'un marché intérieur de l'échange de ce type de données. ».

[863] *Ibid*., p. 6 : « En ce qui concerne l'altruisme en matière de données, l'intervention réglementaire à faible intensité consistait en un cadre de certification volontaire pour les organisations désireuses d'offrir ce type de services, tandis que l'intervention réglementaire à forte intensité prévoyait un cadre d'autorisation obligatoire. ».

[864] *Ibid*., considérant 20, p. 22 : « Une procédure de notification pour les services de partage de données devrait être mise en place afin de garantir que la gouvernance des données au sein de l'Union est fondée sur un échange de données digne de confiance. Le meilleur moyen de tirer avantage d'un environnement digne de confiance serait d'imposer un certain nombre d'exigences pour la prestation de services de partage de données sans pour autant qu'une décision expresse ou un acte administratif ne soient exigés à cette fin de l'autorité compétente. ».

[865] Cassar Bertrand, « Gouvernance des données », Encyclopédie Dalloz : NTIC et IP/IT, 2022.

moyens à mettre en œuvre pour utiliser ces informations dans le respect des personnes protégées[866] ».

310. L'instauration de nouveaux acteurs du système de confiance. Afin de garantir la confiance dans le partage de données à caractère personnel et non personnel, le règlement instaure un nouveau type d'acteurs : les services d'intermédiation de données. Les services d'intermédiation de données deviennent les garants d'un système de partage de confiance[867]. Il s'agit d'un service qui vise à établir des relations commerciales à des fins de partage de données des personnes concernées ou des détenteurs de données avec des utilisateurs de données[868]. Les intermédiaires de données sont les acteurs clés du règlement sur la gouvernance des données. Ils permettent de faciliter l'agrégation et l'échange de quantités substantielles de données dans le but de créer de nouveaux écosystèmes fondés sur les données indépendantes des géants du numérique[869]. Pour cela, ils vont devoir démontrer leur « neutralité économique »[870], c'est-à-dire qu'ils doivent se limiter à leur rôle d'intermédiaire et ce, sans l'ombre d'un potentiel conflit d'intérêts. La neutralité de ces prestataires est indispensable afin de garantir la confiance dans ce partage des données : la neutralité permet de distinguer ces prestataires à l'économie des géants du numérique. Ainsi, les courtiers de données sont naturellement exclus de la catégorie

[866]Cassar Bertrand, « L'importance de la gouvernance des données dans l'usage de systèmes d'IA générative », Dalloz IP/IT, 2023, p. 513.

[867] Hulin Anne-Sophie « La gouvernance des données de l'IA ou l'avènement d'une nouvelle ère normative en droit du numérique », *op. cit*., p. 485.

[868] Règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données, article 2, 11) ; Selon la CNIL : « Les services d'intermédiation de la donnée sont un modèle commercial visé par le Data Governance Act qui a pour objectif de permettre aux entreprises et particuliers de partager des données. Ces services peuvent prendre par exemple la forme de plateformes numériques permettant le libre partage ou contrôle de leurs données par les entreprises et particuliers ainsi que d'exercer leurs droits pour ces derniers. », disponible sur https://www.cnil.fr.

[869] Règlement (UE) 2022/868 du 30 mai 2022 portant sur la gouvernance européenne des données, Considérant 22.

[870] Saillant Clara, « Articulation du RGPD et du DGA : l'analyse économique de la CNIL », Dalloz Actualité, 13 mars 2023.

d'intermédiaires de données[871], étant des acteurs agissant de manière opaque dans un intérêt strictement mercantile[872].

311. L'altruisme des données. Toujours dans le dessein d'une ouverture globale des données, le règlement instaure « l'altruisme des données », c'est-à-dire la mise à disposition volontaire de données, par des particuliers ou des entreprises pour le bien commun, sans contrepartie. Il s'agit d'instaurer dans ce nouvel écosystème de confiance un modèle d'échange « désintéressé » des données[873]. La confiance et le partage deviennent des valeurs communes dans cet écosystème où l'intérêt général prime. Les individus vont partager des données dans un objectif d'amélioration des secteurs de la santé, de la lutte contre le réchauffement climatique, de l'amélioration de la mobilité et des services publics ou encore de la recherche scientifique. Les organismes qui pratiquent l'altruisme des données pourront s'enregistrer en tant qu'organisation altruiste en matière de données reconnues dans l'Union européenne. Toutefois, la logique de ce mouvement reste exclusivement incitative et il faut donc espérer que la dimension incitative soit plus forte que la recherche du profit, ce qui reste à démontrer. À la première lecture, l'approche altruiste du partage des données paraît quelque peu chimérique. Le cas échéant, une intelligence artificielle de confiance pourrait se développer grâce au partage de données.

2. Le développement d'une intelligence artificielle de confiance

312. Les limites du droit souple. Dans le cadre de son approche globale, l'Union européenne a la prétention de développer une intelligence artificielle éthique. Afin de ne pas brider l'innovation en élaborant un cadre normatif trop restreint, le droit européen a dans un premier

[871] Règlement (UE) 2022/868 du 30 mai 2022 portant sur la gouvernance européenne des données, considérant 22 : « Les prestataires de services en nuage devraient être exclus, de même que les prestataires de services qui obtiennent des données auprès de détenteurs de données, les agrègent, les enrichissent ou les transforment et accordent à des utilisateurs de données des licences d'utilisation pour les données qui en résultent, sans établir de relation directe entre les détenteurs de données et les utilisateurs de données, par exemple, les courtiers en publicité ou courtiers de données, les cabinets de conseil en données, les fournisseurs de produits de données résultant de la valeur ajoutée aux données par le prestataire de services. ».
[872] Douville Thibault et Netter Emmanuel, « Présentation critique du Data governance act », RTD com., 2022, pp. 561-574.
[873] Hulin Anne-Sophie, « La gouvernance des données de l'intelligence artificielle ou l'avènement d'une nouvelle ère normative en droit du numérique », *op. cit.*, p. 481.

temps eu principalement recours au droit souple[874] : l'Union européenne a souhaité faire confiance aux acteurs du numérique. En effet, le droit souple permet d'être plus adaptable et surtout, d'être déterritorialisé pour une approche globale. Néanmoins, le respect des chartes éthiques a malheureusement montré ses limites[875] : le droit souple ne permet pas de faire face aux enjeux et aux risques de l'intelligence artificielle[876]. Les acteurs peuvent « privatiser » les normes en défendant leurs propres intérêts[877]. Pire encore, le droit souple en matière d'intelligence artificielle a fait l'objet d'une ineffectivité au regard de l'absence de contrainte. Pour la Professeure Céline Castets-Renard, l'absence de respect de ces chartes est révélatrice d'un « *ethical washing* »[878]. L*'Ethical washing* étant le résultat d'une démarche consciente et délibérée de divulguer de fausses informations au public afin de paraitre plus éthique que la réalité. Les géants du numérique n'hésitent pas à se faire passer publiquement pour des acteurs respectueux des droits des individus, tout en sachant pertinemment ne pas les respecter. Pour d'aucuns, l'autorégulation constitue un véritable « cheval de Troie » pour ces entreprises[879]. Grâce à leurs connaissances techniques et juridiques, ils ont la maîtrise des moindres failles normatives, leur permettant de perpétuer le développement de leurs activités[880].

313. L'entrée en vigueur du Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence

874 Pour une liste d'exemples non exhaustive : Conseil de l'Europe, « La convergence technologique, l'intelligence artificielle et les droits de l'homme », Recommandation 2102 (2017) ; Conseil de l'Europe, Recommandation sur les impacts des systèmes algorithmiques sur les droits de l'homme (CM/Rec (2020)1 ; Conseil de l'Europe, « Lignes directrices sur l'intelligence artificielle et la protection des données », 25 janvier 2019.

875 Pouzet Clémentine, « Le droit aux prises des incertitudes de l'intelligence artificielle », 20èmes Rencontres des Jeunes Chercheurs en Intelligence Artificielle, Juin 2022, Saint-Etienne, France.

876 Eynard Jessica et Castets-Renard Céline « Introduction », *in* Eynard Jessica et Castets-Renard Céline (dir.), *Un droit de l'intelligence artificielle. Entre règles sectorielles et régime général. Perspectives comparées*, éd. Bruylant, 2023, p. 32 : « Ce "mou" normatif ne peut permettre de faire face à l'ampleur des de l'IA et le besoin de juridicité se fait sentir. ».

877 Barbier Hugo, « Intelligence artificielle et éthique », *in* Bensamoun Alexandra et Loiseau Grégoire (dir.), *Droit de l'intelligence artificielle*, éd. LGDJ, 2022, p. 11 : « La confiscation de la norme par des acteurs influents à même de produire un droit souple fortement diffusé constitue l'un des dangers les plus graves de l'éthique de l'IA portée par des instruments de droit souple. ».

878 Castets-Renard Céline, « Comment construire une intelligence artificielle responsable et inclusive ? », Recueil Dalloz 2020 p. 225.

879 Poullet Yves, « "La troisième voie", une voie difficile. Quelques réflexions autour de la politique européenne en matière d'intelligence artificielle », Revue Lamy Droit de l'Immatériel, n° 182, 1er juin 2021, p. 6.

880 Bensamoun Alexandra et Masmi-Dazi Fayrouze, « Intelligence artificielle : pour l'émergence d'un écosystème européen éthique et compétitif », LexisNexis, La semaine juridique, n° 3, 22 janvier 2024.

artificielle. De fait, l'Union européenne récemment choisi la voie réglementaire pour réguler l'intelligence artificielle[881]. Le règlement sur l'intelligence artificielle a définitivement été adopté le 21 mai 2024 et son entrée en vigueur est prévue pour 2026. Avec ce règlement, l'Union européenne devient pionnière en matière de régulation d'intelligence artificielle[882]. Le règlement sur l'intelligence artificielle met fin en partie à l'ère de l'autorégulation pour le développement de cette technologie et constitue un « acte d'autorité[883] ». La démonstration d'autorité de l'Union européenne s'illustre avec le montant des amendes administratives : jusqu'à 35 000 000 euros ou 7% du chiffre d'affaires en présence d'une entreprise. Naturellement, la promotion de l'intelligence artificielle passe par le développement d'une intelligence artificielle de confiance.

314. Intelligence artificielle digne de confiance. Afin d'établir une intelligence artificielle digne de confiance, l'éthique va constituer une sorte de boussole pour le législateur dans le dessein de promouvoir l'innovation tout en minimisant les risques[884]. Depuis toujours, le développement des technologies ouvre de nouvelles interrogations, voire problématiques. L'éthique apparaît comme un indispensable afin d'assurer une cohérence entre l'innovation et les risques, selon des modèles de sociétés divergents. Dès 1993, Guy Bourgeault écrivait « la technologie ouvre le champ de l'éthique en renforçant une maîtrise humaine sur le monde […]. La conscience des pouvoirs nouveaux conférés par le développement d'une technologie marque de façon radicale l'expérience éthique contemporaine : elle exige du même coup une révision du droit : de ses repères et de ses fondements[885]. ». Pour l'intelligence artificielle, l'éthique doit guider une responsabilité solidaire de tous les acteurs ayant ces outils dans les mains. Les acteurs développant ces outils doivent respecter les droits et libertés fondamentaux instaurés

881 Sénéchal Juliette, « Vote des parlementaires européens sur l'AI Act : vers une réglementation accrue des IA, des modèles de fondation et des IA génératives, s'inspirant du DSA, du Data Act et du RGPD ? », Dalloz Actualités, 22 juin 2023.

882 Ancel Bruno, « L'intelligence artificielle au XXIe siècle : outil juridique fiable ou amplificateur d'injustices ? », LPA, 31 mai 2024.

883 Bertrand Brunessen, « La politique de l'Union européenne en matière d'intelligence artificielle : entre approche sectorielle et transversale », *in* Eynard Jessica et Castets-Renard Céline (dir.), *Un droit de l'intelligence artificielle. Entre règles sectorielles et régime général. Perspectives comparées*, éd. Bruylant, 2023, p. 74.

884 Godefroy Lémy, « Les figures de l'éthique en droit européen de l'intelligence artificielle », *in* Eynard Jessica et Castets-Renard Céline (dir.), *Un droit de l'intelligence artificielle. Entre règles sectorielles et régime général. Perspectives comparées*, éd. Bruylant, 2023.

885 Bourgeault Guy, « L'éthique et le droit aujourd'hui : quand les fondations sont ébranlées... », Les cahiers de droit, 34, pp. 531.

depuis plusieurs décennies. À chaque instant, l'éthique doit être privilégiée face aux gains financiers. En réalité, les acteurs détenant une avance sur ces technologies sont en partie les géants du numérique et s'ils décident de ne pas être guidés par l'éthique, il sera difficile de prouver que ce n'est pas le cas, ou du moins il sera sûrement trop tard[886]. Autrement dit, en matière d'éthique, les comportements doivent être à l'opposé de ceux des géants du numérique en matière de données.

315. Accès aux données. Finalement, la confiance n'est pas synonyme d'éthique : l'éthique est le moyen de développer une intelligence artificielle de confiance[887]. L'éthique permet de rendre socialement acceptable une pratique crainte par la société[888]. En ce sens, l'éthique profite aux géants du numérique rendant des pratiques socialement acceptées. Tel est le cas de l'agent conversationnel basé sur de l'intelligence artificielle « ChatGPT », craint dans un premier temps et finalement utilisé par une majorité d'individus. Pour développer ces technologies, les acteurs concernés doivent avoir accès aux données : « l'algorithme sans données est aveugle. Les données sans algorithmes sont muettes[889] ». Ainsi, l'accès aux données a été privilégié avec les récents règlements : l'inclusion des enjeux de l'intelligence artificielle dans chaque règlement permet aux acteurs d'avoir accès à une masse satisfaisante de données afin de pouvoir développer leurs systèmes d'intelligence artificielle[890]. Les récents règlements participent à l'élaboration d'un écosystème de confiance au sein duquel peut s'affirmer une intelligence artificielle de confiance. Les acteurs vont avoir accès aux données à caractère non personnel en général et plus spécifiquement, aux données publiques ouvertes, aux données industrielles ou encore aux données d'intérêt général etc. L'importance de la quantité des

[886] *Ibid*., p. 532 : « À l'opposé, d'autres, depuis plus de 20 ans encore, soutiennent que la technologie, si elle n'est pas "humanisée" par ses utilisateurs ou si ceux-ci, usant inconsidérément des pouvoirs nouveaux qui leur sont dévolus, continuent de jouer les apprentis sorciers, conduira l'humanité entière à sa perte ; et le cosmos, avec elle, à la catastrophe ».

[887] Poullet Yves, « "La troisième voie", une voie difficile. Quelques réflexions autour de la politique européenne en matière d'intelligence artificielle », Revue Lamy Droit de l'Immatériel, n° 182, 1er juin 2021.

[888] Godefroy Lémy, *op. cit*.

[889] Commission nationale de l'informatique et des libertés, « Comment permettre à l'homme de garder la main ? Les enjeux éthiques des algorithmes et de l'intelligence artificielle », Rapport, p. 18.

[890] Delmas-Linel Béatrice et Dumas Grégoire, « L'impact du RGPD sur les innovations en matière d'IA », *in* G'Sell Florence (dir.), *Le Big Data et le Droit,* éd. Dalloz, 2020, p. 208 : « Tout l'enjeu de l'IA tient d'ailleurs à l'accès et au partage des données. », qui cite une étude réalisée par Atawao Consulting et publiée par PIPAME, « Prospective Intelligence artificielle : état de l'art et perspectives pour la France », février 2019.

données n'est plus à démontrer dans le développement des systèmes fiables[891]. À nouveau, le concept de confiance devient un élément majeur de l'accès aux données : lorsque les acteurs auront confiance et accès aux données, l'Europe pourra devenir un acteur incontournable en matière d'intelligence artificielle.

316. Qualité des données. En outre, la confiance est également liée à la qualité des données. La nécessité de la qualité des données n'est pas un paramètre récent. En matière d'innovation, la qualité des données est une caractéristique indispensable pour faciliter les flux de données. Les flux vont pouvoir être aisés lorsque les données sont annotées afin d'être exploitables[892]. En revanche, lorsque les données sont de mauvaise qualité, le traitement des données va nécessiter des coûts importants. Ainsi, les règlements précités insistent sur la qualité des données par la notion de gouvernance des données[893]. À titre d'illustration, le règlement sur les données anticipe et harmonise les règles sur l'interopérabilité des données.

Le règlement sur la gouvernance des données quant à lui permet la facilitation du partage des données entre les entreprises et les pouvoirs publics dans l'intérêt public et « contribuera à fournir un accès fiable, responsable et non discriminatoire à des données de haute qualité pour l'entraînement à des données de haute qualité pour l'entraînement, la validation et le test des SIA[894]. ». Quant au règlement sur l'intelligence artificielle, ce dernier insiste également sur l'importance de la qualité des données : l'accès et la qualité des données jouent un rôle primordial. Lorsqu'un système d'intelligence artificielle à haut risque est entraîné avec un modèle se basant des données, les jeux de données sont soumis à des pratiques appropriées en

[891] Mouncif-Moungache Mouna, « Le règlement sur la gouvernance des données ou l'émergence d'un modèle européen », *in* Eynard Jessica et Castets-Renard Céline (dir.), *Un droit de l'intelligence artificielle. Entre règles sectorielles et régime général. Perspectives comparées*, éd. Bruylant, 2023, p. 508 : « Les données doivent être davantage partagées entre les acteurs qui utilisent des données afin de promouvoir les innovations de tous ordres et permettre à l'intelligence artificielle de s'alimenter grâce à ces données d'entraînement de plus en plus riches et diverses. ».

[892] Bertrand Brunessen, « La gouvernance des données dans la régulation européenne de l'intelligence artificielle », RTDeur., Revue trimestrielle de droit européen, 2022, 03, p. 315 ; Ollier Jean-Yves, « La gouvernance européenne des données », *in* Bertrand Brunessen (dir.), *La politique européenne du numérique*, éd. Bruylant, 2023, p. 735.

[893] Truck Isis, « Données et responsabilité du point de vue de l'informaticien », *in* Bévière-Boyer Bénédicte, Dibie Dorothée et Arlotti Clément (dir.), *Numérique, droit et société*, éd. Dalloz, 2022, p. 215.

[894] Proposition de règlement du parlement européen et du conseil établissant des règles harmonisées concernant l'intelligence artificielle (législation sur l'intelligence artificielle) et modifiant certains actes législatifs de l'union, COM(2021) 206 final, Considérant 45.

matière de gouvernance des données[895]. En réalité - et pour le moment -, ce sont principalement les géants du numérique qui détiennent les moyens de développer des données de qualité. Étant les possesseurs de la majorité des données, ils détiennent le pouvoir de décider du partage de données de qualité ou volontairement, de données biaisées.

317. Biais et discrimination. Logiquement, la qualité des données détermine la qualité de la décision : la qualité dépend de la représentativité ou biais des données initiales[896]. Lorsque des biais se cachent dans les jeux de données du modèle ou de l'algorithme, les risques pour les individus sont prégnants, notamment en matière de discrimination[897]. Il peut s'agir de risques générés par des algorithmes d'aides à la décision comme la prise de décision pour l'attribution d'un logement ou d'un avantage[898]. En matière d'intelligence artificielle, la difficulté résulte du caractère difficilement décelable des discriminations formées par les systèmes d'intelligence artificielle et par conséquent, de les corriger ou de les supprimer[899]. Les risques sont d'autant plus prégnants dans les systèmes d'intelligence artificielle à haut risque : « les conséquences d'une intelligence artificielle qui n'a pas été entrainée avec des données d'une qualité suffisante peut se révéler dramatiques[900] ». Par ailleurs, l'ouverture des données par l'Union européenne est un objectif important d'un point de vue économique. En revanche, l'ouverture excessive des données comporte des risques pour les individus.

II. Les conséquences de l'ouverture excessive des données

318. Altération protection et essor des risques. Du point de vue de l'innovation, le dessein de l'Union européenne d'ouvrir les données afin de développer l'intelligence artificielle est louable. Néanmoins, l'ouverture excessive des données entraîne progressivement une altération de la protection des données à caractère personnel (A). De surcroît, il faudra être très attentif

[895] *Ibid*., article 10, point 1 : « Les systèmes d'IA à haut risque faisant appel à des techniques qui impliquent l'entraînement de modèles au moyen de données sont développés sur la base de jeux de données d'entraînement, de validation et de test qui satisfont aux critères de qualité visés aux paragraphes 2 à 5. ».
[896] Besse Philippe, Castets-Renard Céline, GarivierAurélien *et al.*, « L'IA du Quotidien peut elle être Éthique ? », Loyauté des Algorithmes d'Apprentissage Automatique, 2018.
[897] Latil Arnaud, *Le droit du numérique. Une approche par les risques,* éd. Dalloz, 2023.
[898] Castets-Renard Céline, *Droit du marché unique numérique et intelligence artificielle*, éd. Bruylant, 2020, p. 334.
[899] Loiseau Grégoire « Intelligence artificielle et droit des personnes », *in* Bensamoun Alexandra et Loiseau Grégoire (dir.), *Droit de l'intelligence artificielle*, éd. LGDJ, 2022, p. 49.
[900] Bertrand Brunessen, *op. cit*.

aux conséquences des systèmes d'intelligence artificielle à haut risque sur les droits des individus. En effet, certaines promesses de protection semblent désormais chimériques (B).

A) L'altération progressive de la protection des données à caractère personnel

319. Adaptation des principes de protection. Par-delà les titres protecteurs des récents règlements, l'Union européenne ne dissimule pas son ambition d'ouvrir les flux de données afin de libérer le potentiel des données (1). À cette fin, elle n'hésite pas à adapter certaines interdictions au nom de l'innovation (2).

1. La primauté du potentiel économique sur les enjeux de protection

320. L'innovation au nom de la protection. L'accès aux données est un préalable inéluctable au développement des systèmes d'intelligence artificielle, les données étant la matière première de l'intelligence artificielle[901]. Pour ce faire, l'Union européenne a renforcé l'ouverture et l'accès des données à caractère non personnel afin de stimuler l'innovation. Le modèle de gouvernance des données apparaît comme divergent au modèle instauré par le Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données[902]. L'Union européenne œuvre pour tenter de concevoir un équilibre entre innovation et protection des données à caractère personnel et l'illustration objective de cette tentative de conciliation se trouve dans la double base juridique du règlement sur l'intelligence artificielle : l'article 114 sur le fonctionnement du marché intérieur[903] et l'article 16 sur la protection des données à caractère personnel[904].

---

901 *Ibid*.

902 Sénéchal Juliette, « L'IA Act déjà obsolète face aux IA de nouvelle génération ? », Dalloz Actualité, 1er février 2023.

903 Traité sur le fonctionnement de l'Union européenne (TFUE), article 1114.

904 *Ibid.*, article 16 point 1) : « 1. Toute personne a droit à la protection des données à caractère personnel la concernant. ».

L'ouverture des données a toujours été priorisée par l'Union européenne afin d'anticiper le développement de l'intelligence artificielle[905]. Dès le règlement sur la protection des données à caractère personnel, l'article premier précise que « la libre circulation des données à caractère personnel au sein de l'Union n'est ni limitée ni interdite pour des motifs liés à la protection des personnes physiques à l'égard du traitement des données à caractère personnel[906] ». Par ailleurs, les récents règlements - le règlement sur la gouvernance des données, sur les données ou encore sur l'intelligence artificielle - « sacrifient » les principes de protection des données à caractère personnel[907]. Ainsi, malgré l'entière attention portée sur le caractère protecteur du règlement sur la protection des personnes à l'égard de leurs données, certaines dispositions attestent de la priorité portée à la libre circulation des données, qu'elles soient personnelles ou non personnelles. À titre d'illustration, les « bacs à sable réglementaire » vont permettre à ces acteurs de développer des technologies sans respecter la législation.

321. Bac à sable réglementaire. Il sera possible, de manière temporaire certes, de tester des technologies sans respecter l'ensemble des règles applicables[908]. L'élaboration de « bacs à sable règlementaires » contribue à cette priorisation de l'innovation sur la protection en permettant l'usage de données à caractère personnel de façon « sécurisée »[909]. La Commission nationale de l'informatique et des libertés confirme par ailleurs que le développement des systèmes d'intelligence artificielle implique l'utilisation de volumes importants de données à caractère personnel, issues de sources variées[910]. Il nous semble nécessaire de veiller à l'importance de l'effectivité du cadre normatif protecteur des données à caractère personnel et de ne pas anéantir la protection des utilisateurs au nom de l'innovation[911]. Finalement, ce sont à nouveau les géants

---

905 Bordais Pierre, « L'autodétermination informationnelle à l'épreuve des évolutions technologiques », Dalloz IP/IT, 2024, p. 72 : « La tendance générale est davantage à l'ouverture des données qu'à la fermeture de celles-ci. Rien d'étonnant, le RGPD lui-même mentionne dans son intitulé qu'il poursuit un objectif de libre circulation de la donnée. En ce sens, l'open data se développe énormément depuis une dizaine d'années. ».

906 Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, article 1.

907 Poullet Yves, « Cinq ans après - le RGPD est-il toujours la solution ? », RDTI, n° 90, 2023, p. 12.

908 Petel Antoine, « Quel bilan normatif pour l'Europe numérique ? », LexisNexis, Europe, n° 5, mai 2024.

909 Cassar Bertrand, « L'importance de la gouvernance des données dans l'usage de systèmes d'IA générative », Dalloz IP/IT, 2023, p. 513.

910 Commission nationale de l'informatique et des libertés, « "Les bacs à sable" données personnelles : la CNIL lance un appel à projets sur l'intelligence artificielle dans les services publics », 21 juillet 2023, disponible sur : https://www.cnil.fr.

911 Foucart Romain, « Acte fondateur ou coup d'épée dans l'eau ? Observations relatives à la stratégie européenne pour les données », Revue de l'Union européenne, n° 647, p. 217 : « Si l'encadrement de l'utilisation de données, appelée à se généraliser et à se densifier, est fondamental et ne peut être envisagé

du numérique qui vont profiter de l'ouverture des données pour entraîner leurs systèmes d'intelligence artificielle.

2. L'adaptation à risque des principes protecteurs au nom de l'innovation

322. L'incompatibilité des principes protecteurs des données à caractère personnel pour le développement de l'intelligence artificielle. À la lecture du règlement sur la protection des données à caractère personnel, il est possible de déceler l'incompatibilité des principes protecteur pour le développement de l'intelligence artificielle. En effet, les responsables de traitement doivent respecter les principes tels que le principe de minimisation ou encore de finalité[912]. D'une façon pragmatique, le règlement sur la protection des données à caractère personnel a été mis en place au regard des risques pour les individus[913] et constitue un obstacle au développement de ces technologies. Pourtant, il est nécessaire que les responsables de traitement respectent ces principes protecteurs, la protection des données à caractère personnel étant un enjeu majeur dans le développement de l'intelligence artificielle[914] : certains systèmes d'intelligence artificielle utilisés par les géants du numérique dans l'intention de manipuler les comportements nécessitent une collecte généralisée et une conservation prolongée de données à caractère personnel[915]. En réalité, les pratiques de certains acteurs afin d'entraîner leurs

sans la règle de droit, il importe cependant que dans son entreprise de rattrapage, l'Union ne remette pas en cause son modèle de société sous pretexte de se mettre à niveau. ».

912 Perray Romain, «Données à caractère personnel. Principes fondamentaux relatifs aux traitements de données à caractère personnel. Limitation des finalités : JCl. Administratif, fasc. 274-22, à paraître et JCl. Communication, fasc. 932-20 ; Perray Romain « Données à caractère personnel. Principes fondamentaux relatifs aux traitements de données à caractère personnel. Minimisation » : JCl. Administratif, fasc. 274-23 et JCl. Communication , fasc. 932-30.

913 Bensamoun Alexandra et Zolynski Célia, « Big data et privacy : comment concilier nouveaux modèles d'affaires et droits des utilisateurs ? », LPA, 16 août 2014, 162, pp. 8-12.

914 Lequette Suzanne, *Droit du numérique*, éd. LGDJ, 2024, p. 769 : « La protection des données à caractère personnel est un enjeu majeur du droit de l'intelligence artificielle au regard du traitement massif et bien souvent opaque des données qu'elle opère. ».

915 Vergnolle Suzanne, « L'illusoire interdiction des pratiques manipulatoires dans le projet de règlement sur l'intelligence artificielle », *in* Eynard Jessica et Castets-Renard Céline (dir.), *Un droit de l'intelligence artificielle. Entre règles sectorielles et régime général. Perspectives comparées*, éd. Bruylant, 2023, p. 440.

systèmes d'intelligence artificielle contreviennent directement aux principes du règlement sur la protection des données à caractère personnel[916].

323. Directives de la CNIL. Ainsi, afin de concilier – ou plutôt d'anéantir - les principes antinomiques à l'innovation, la Commission nationale de l'informatique et des libertés a dévoilé ses premières réponses à une intelligence artificielle innovante et respectueuse de la vie privée. En effet, le principe de finalité impose au responsable de traitement de données à caractère personnel de déterminer à l'avance l'objectif du traitement. En réalité, le principe de finalité n'est pas adapté aux systèmes évolutifs d'intelligence artificielle[917]. Pourtant, dans les lignes de sa réponse, la Commission nationale de l'informatique et des libertés admet qu'en matière d'intelligence artificielle, il est possible de ne pas déterminer à l'avance la finalité d'utilisation des données à caractère personnel[918]. Il s'agirait d'un principe de finalité « adapté » pour le développement de l'intelligence artificielle. De surcroît, toujours selon la CNIL, le principe de minimisation n'empêcherait pas l'entraînement d'algorithmes sur des « très grands ensemble de données ». À force « d'adapter » les principes fondamentaux du règlement sur la protection des données à caractère personnel au nom de l'innovation, les principes de protection deviendront chimériques. Il nous semble que l'Union européenne a fait le choix de développer les intérêts économiques des données au détriment de la protection des données à caractère personnel, ce qui est regrettable.

B) La protection chimérique des utilisateurs contre les SIA à haut risque

[916] Poullet Yves, « Cinq ans après : le RGPD et les défis du profilage à l'heure de l'intelligence artificielle », Revue des affaires européennes, numéro 1, pp. 87-101.

[917] Poullet Yves, *Le RGPD aux défis de l'intelligence artificielle*, éd. Larcier, 2020, p. 69 : « Le respect du principe de finalité déterminée pose donc une difficulté face à des systèmes d'information, complexes, sans cesse évolutifs et capables, au gré du fonctionnement d'un système d'IA, de se voir assigner de nouvelles tâches liées aux opportunités du machine learning. Cette possibilité d'évolution des finalités, offerte par la technologie du machine learning, renvoie aux limites de ce qu'il faut entendre par une "finalité compatible". ».

[918] Commission nationale de l'informatique et des libertés, « Intelligence artificielle : la CNIL dévoile ses premières réponses pour une IA innovante et respectueuse de la vie privée », 11 octobre 2023 : « Le principe de finalité impose de n'utiliser des données personnelles que pour un objectif précis (finalité) défini à l'avance. En matière d'IA, la CNIL admet qu'un opérateur ne puisse pas définir au stade de l'entraînement de l'algorithme l'ensemble de ses applications futures, à condition que le type de système et les principales fonctionnalités envisageables aient été bien définies. ».

324. L'appréhension technique de l'environnement numérique. Dans un environnement technique difficile à appréhender pour les juristes, les géants du numérique ont encore la possibilité de rendre chimérique le principe de transparence. Les nouvelles technologies sont de plus en plus autonomes et par conséquent, de plus en plus difficilement interprétable par un humain. Dès lors, le principe de transparence imposé par le règlement sur l'intelligence artificielle paraît utopique (1), affaiblissant la protection promue pour les utilisateurs (2).

1. L'utopique principe de transparence

325. Principe de transparence. Afin de protéger les individus contre les risques, le principe de transparence est instauré dans le règlement sur l'intelligence artificielle[919]. Le rapport Villani précisait déjà que « l'explicabilité de ces technologies est l'une des conditions de leur acceptabilité sociale. (…) En effet, sans possibilité d'expliquer les décisions prises par des systèmes autonomes, il apparaît difficile de les justifier[920]. ». Les concepteurs d'outils d'intelligence artificielle doivent être en mesure d'expliquer le fonctionnement de leurs outils[921]. Le processus d'apprentissage des systèmes devient fondamental pour expliquer leur fonctionnement. Pour cela, il est nécessaire de conserver les données d'apprentissage tout en respectant les dispositions en termes de gouvernance des données et surtout, en matière de protection des données à caractère personnel si nécessaire. La transparence relève d'une logique de *compliance*. Dès lors que les systèmes d'intelligence artificielle sont susceptibles d'impacter les individus, il revient aux concepteurs d'outils d'expliquer leurs outils en mettant en place des procédures internes afin de respecter la gouvernance des données[922]. La transparence est un gage

---

919 Proposition de règlement du parlement européen et du conseil établissant des règles harmonisées concernant l'intelligence artificielle (législation sur l'intelligence artificielle) et modifiant certains actes législatifs de l'union, COM(2021) 206 final, article 13 : Transparence et fourniture d'informations aux déployeurs « 1. La conception et le développement des systèmes d'IA à haut risque sont tels que le fonctionnement de ces systèmes est suffisamment transparent pour permettre aux déployeurs d'interpréter les sorties d'un système et de les utiliser de manière appropriée. Un type et un niveau adéquats de transparence sont garantis afin de veiller au respect des obligations pertinentes incombant au fournisseur et au déployeur énoncées à la section 3. ».

920 Villani, « Donner un sens à l'intelligence artificielle », Rapport, 28 mars 2018, issu de la mission parlementaire sur la mise en œuvre d'une stratégie francaise et européenne en intelligence artificielle, p. 140.

921 Bensamoun Alexandra et Masmi-Dazi Fayrouze, « Intelligence artificielle : pour l'émergence d'un écosystème européen éthique et compétitif », LexisNexis, La semaine juridique, n° 3, 22 janvier 2024, p. 143 : « Sans obligation de transparence via le partage des données et l'interopérabilité, ce sont les opérateurs déjà puissants, verticalement et conglomeralement intégrés, qui captent l'innovation, soit en l'internalisant, soit en la neutralisant. ».

922 Bertrand Brunessen, « La gouvernance des données dans la régulation européenne de l'intelligence artificielle », *op. cit*.

de fiabilité pour les individus et lorsqu'ils interagissent avec des systèmes d'intelligence artificielle, ils doivent pouvoir être en mesure de conserver leur autodétermination « totale et effective[923] ». La transparence permettrait aux systèmes d'intelligence artificielle d'être compréhensibles et par conséquent, contrôlables par les individus[924].

326. Opacité des systèmes d'intelligence artificielle. En réalité, les systèmes d'intelligence artificielle sont souvent inintelligibles[925] : ils sont autoapprenants et difficilement explicables par l'humain[926]. Par conséquent, l'obligation de transparence imposée apparaît chimérique[927]. Les lacunes au sujet de l'explicabilité des systèmes impactent directement les principes de transparence[928]. Dans certains cas, il est compliqué de procéder à l'effacement des données. Pour les intelligences artificielles génératives, il peut y avoir « un risque sur l'exactitude des données, parce que c'est un système probabiliste qui n'est pas nécessairement fiable[929] ». Ces dernières vont traiter les données à caractère personnel plusieurs fois dans leur cycle de vie, il sera alors difficile de vérifier si les données ont réellement été effacées. Les algorithmes se servent généralement sur les données déjà accessibles et les utilisateurs sont souvent inconscients de la possession de certaines de leurs données par certains acteurs.

---

923 Commission européenne, « Lignes directrices en matière d'éthique pour une IA digne de confiance », avril 2019, p. 15 : « Les droits fondamentaux sur lesquels l'UE est fondée ont vocation à garantir le respect de la liberté et de l'autonomie des êtres humains. Les êtres humains qui interagissent avec des systèmes d'IA doivent être en mesure de conserver leur autodétermination totale et effective et de prendre part au processus démocratique. ».

924 Bensamoun Alexandra et Loiseau Grégoire, « L'intelligence artificielle à la mode éthique », Recueil Dalloz, 2017, n°24, p. 1371.

925 Poullet Yves, « Consent : "The privacy bug" », La confiance numérique : travaux de la Chaire sur la confiance numérique, LexisNexis, p. 113 : « Ces exigences posent également problème à l'heure d'une intelligence artificielle opaque et aux finalités difficilement circonscrites. ».

926 Castets-Renard Céline, « Nouvelles technologies et droit européen : quel droit face à l'intelligence artificielle ? », *in* Sylvie Peyrou-Bartoll (dir.), *Nouvelles technologies et droit européen : quel droit face à la disruption numérique ?*, éd. Mare et Martin, 2022, p. 13 : « La rencontre entre le droit et la technique n'est pas nouvelle, mais les intelligences artificielles peuvent vite donner le tournis, dès lors que l'on évoque leur opacité et complexité. » .

927 Delmas-Linel Béatrice et Dumas Grégoire, *op. cit.*, p. 213.

928 Arlotti Clément, « Éthique computationnelle : un oxymore ? Les approches contractualistes de la philosophie du risque au secours de l'intelligence artificielle », *in* Bévière-Boyer Bénédicte, Dibie Dorothée et Arlotti Clément (dir.), *Numérique, droit et société*, éd. Dalloz, 2022, p. 328 : « Idéalement, chaque trace d'exécution d'un système autonome éthique devrait pouvoir être associée, par un mécanisme explicable, à un état connu et interprétable par la machine. Or, ce n'est pas toujours le cas pour un algorithme d'apprentissage : ce sont les fameux problèmes de "l'explicabilité" et de "l'interprétabilité". ».

929 Denis Marie-Laure, Présidente de la Cnil, entretien pour l'AFP.

Pour l'instant, il est difficile d'appréhender la manière dont les concepteurs vont pouvoir remplir leur obligation de transparence, qui plus est en présence d'une technologie fortement évolutive[930]. L'opacité des systèmes d'intelligence artificielle est également renforcée par l'asymétrie d'information - voire d'accès - entre les responsables du code et les responsables chargés du contrôle[931]. La technicité de la programmation permet de faire perdurer certaines technologies au regard du temps nécessaire à l'élaboration des normes. En pratique, « plus les individus sont transparents, plus ceux qui les observent sont opaques[932] ». L'opacité de ces pratiques entraîne une protection utopique des individus.

2. L'utopique protection des individus

327. Interdiction de certains systèmes d'IA. L'usage et le développement des systèmes d'intelligence artificielle entraînent des risques amplifiés pour les individus[933] : le fait que ces systèmes interagissent avec les êtres humains accroît les risques d'atteinte à la personne[934]. À titre d'illustration, l'article 5.1 du règlement sur l'intelligence artificielle interdit plusieurs pratiques d'intelligence artificielle présentant un risque d'atteinte inacceptable aux droits fondamentaux des individus. Il peut s'agir d'un système d'intelligence artificielle ayant recours à des techniques subliminales ou à des techniques délibérément manipulatrices ou trompeuses ayant pour objectif ou effet d'altérer le comportement d'un groupe ou d'une personne en portant atteinte à la capacité de prendre une décision pouvant lui causer un préjudice[935].

---

930 Sirinelli Jean et Bertrand Brunessen, « L'approche comportementale dans la régulation du numérique, Bertrand Brunessen et Sirinelli Jean », *Mélanges en l'honneur de Pierre Sirinelli*, éd. Dalloz, 2022, p. 595.

931 Prevost Jean-Baptiste, « La fabrique des données : à propos du codage numérique du droit et de ses limites », Lextenso, Gazette du Palais, mardi 22 janvier 2019, n° 3, p. 83 : « Mais la langue du code et la langue de la programmation (et donc le cœur des algorithmes) sont au contraire fondamentalement inaccessibles au commun des mortels, et les juristes n'ont aucun contrôle direct de la juste transcription de leur savoir dans les programmes que les ingénieurs élaborent. […] Le caractère inaccessible de ce langage (celui des programmes des algorithmes) est par conséquent un immense problème : comment accéder à la "vérité", aux fonctions réelles, et à l'intelligibilité interne de ces programmes sachant que le code possède une dimension cryptique pour la plupart d'entre nous ? ».

932 Cardon Dominique, *À quoi rêvent les algorithmes*, éd. La République des idées Seuil, 2015, p. 79.

933 Debet Anne, *op. cit*., p. 335.

934 Loiseau Grégoire, *op. cit*.

935 Proposition de règlement du parlement européen et du conseil établissant des règles harmonisées concernant l'intelligence artificielle (législation sur l'intelligence artificielle) et modifiant certains actes législatifs de l'union, COM(2021) 206 final, article 5.1 a) : « la mise sur le marché, la mise en service ou l'utilisation d'un système d'IA qui a recours à des techniques subliminales au-dessous du seuil de conscience d'une personne pour altérer substantiellement son comportement d'une manière qui cause ou est susceptible de causer un préjudice physique ou psychologique à cette personne ou à un tiers ; ».

Toujours dans le dessein de manipuler le comportement des individus, sont également interdites la mise en service ou l'utilisation d'un système d'intelligence artificielle qui exploite les vulnérabilités dues à l'âge, au handicap ou à la situation économique ou sociale d'une personne ou d'un groupe[936]. Par ailleurs, les systèmes d'intelligence artificielle portant sur l'évaluation ou la classification des personnes physiques au cours d'une période en fonction de leur comportement ou de leurs caractéristiques personnelles permettant l'élaboration d'une note sociale sont interdits. Pour finir, les techniques de profilage afin de prédire le comportement d'une personne physique, les systèmes d'intelligence artificielle de reconnaissance faciale développés à partir de base de données provenant de l'internet ou de la vidéosurveillance ou encore les systèmes destinés à inférer les émotions d'une personne physique sur le lieu de travail ou dans les établissements d'enseignements sont logiquement interdites.

328. Réalité des risques. Toutes ces interdictions pourraient être seulement inspirées de la science-fiction et n'être que des risques inconcevables. Malheureusement, certains risques évoqués dans les interdictions sont une réalité. Par exemple, l'usage du crédit social et l'analyse des émotions au sein du milieu scolaire sont pratiques courantes en Chine. En effet, dans le milieu scolaire, un système de reconnaissance faciale analyse les émotions des élèves à travers leurs expressions de visage. L'analyse des émotions permettrait à l'enseignant d'adapter sa pédagogie selon l'implication des élèves. Quant à la pratique du crédit social, il s'agit pour le gouvernement chinois d'attribuer une note d'honnêteté et de loyauté à partir de données collectées telles que les données commerciales, les médias sociaux ou encore les données de surveillance. L'attribution de cette note va être constitutive de droits, de récompenses ou de

[936] *Ibid*., article 5.1 b) : « la mise sur le marché, la mise en service ou l'utilisation d'un système d'IA qui exploite les éventuelles vulnérabilités dues à l'âge ou au handicap physique ou mental d'un groupe de personnes donné pour altérer substantiellement le comportement d'un membre de ce groupe d'une manière qui cause ou est susceptible de causer un préjudice physique ou psychologique à cette personne ou à un tiers. ».

sanction[937]. Pour d'aucuns, ce système est une simple évolution des pratiques américaines concernant les crédits à la consommation au début des années 2010[938].

329. Superficialité de la protection. Ainsi, l'Union européenne se saisit des risques inspirés par nos lointains voisins afin d'anticiper tout développement néfaste pour les droits fondamentaux des individus. Particulièrement, il s'agit d'encadrer les pratiques manipulatoires qui sont déjà courantes en Europe : les géants du numérique usent de ces pratiques afin que les consommateurs utilisent leurs services et plateformes et ce, le plus souvent et le plus longtemps possible. Pourtant, le règlement ne vise que les recours à des techniques subliminales au-dessous du seuil de conscience de la personne ou l'exploitation des vulnérabilités dues à l'âge ou au handicap physique ou mental d'une personne physique. Néanmoins, plusieurs pratiques courantes des géants du numérique ont pour objet de manipuler le comportement des individus sans qu'ils en aient nécessairement conscience[939]. À titre d'illustration, les pratiques intrusives de publicité ciblée ou de recommandations ne sont pas visées par le texte[940]. Pire encore, les pratiques d'économie de l'attention sont des pratiques qui manipulent le comportement des individus[941]. À nouveau, le règlement est ambitieux mais ne va pas assez loin pour sanctionner

---

937 Lesueur Jean-Thomas, « Le système de crédit social : comment la Chine évalue, récompense et punit sa population », sur Institut Thomas More, publié le 29 juillet 2019 : « L'âge d'or de l'algorithme : le crédit social et la financiarisation de la gouvernance en Chine », Action publique. Recherche et pratiques, 3, Institut de la gestion publique et du développement économique (IGPDE), 2019 ; Il existe depuis plusieurs années déjà dans certaines villes des systèmes de notation chiffrée des citoyens. Celui de Rongcheng, dans le Shandong, est peut-être le plus abouti aujourd'hui. Il établit six catégories possibles, en fonction du nombre de points possédés par chacun :
AAA (plus de 1050 points) : citoyen exemplaire
AA (entre 1030 et 1049 points) : citoyen excellent
A (entre 960 et 1029 points) : citoyen honnête
B (entre 850 et 959) : relativement honnête
C (entre 600 et 849) : niveau d'avertissement
D (549 et moins) : malhonnêteté... », disponible en ligne.

938 Loubere Nicholas, « L'âge d'or de l'algorithme : le crédit social et la financiarisation de la gouvernance en Chine », Action publique. Recherche et pratiques, 3, Institut de la gestion publique et du développement économique (IGPDE), 2019.

939 Castets-Renard Céline, *op. cit.*, p. 18 : « Les circonstances [de l'article 5 du règlement] sont tellement spécifiques qu'elles laisseront de côté l'usage des systèmes d'intelligence artificielle dans des circonstances voisines, dont les effets seront tout aussi dangereux pour les individus et qui seront qualifiés à "haut risque" sans être interdits. ».

940 Vergnolle Suzanne, *op. cit*., p. 462.

941 Peyrou-Bartoll Sylvie, « Quelques réflexions sur les réponses institutionnelles européennes en matière d'intelligence artificielle (IA) et de robots », *in* Peyrou-Bartoll Sylvie, *Nouvelles technologies et droit européen : quel droit face à la disruption numérique ?*, éd. Mare et Martin, 2022, p. 49.

les géants du numérique. Ils disposent des moyens de contourner les normes et la logique de responsabilisation n'est pas adéquate.

Ainsi, la notion de technique subliminale restreint drastiquement le champ d'application de cette mesure. Les techniques de manipulation « visibles » - pour une très faible proportion d'individus - ne seront pas visées par cette interdiction, et cela est regrettable. Par conséquent, les géants du numérique disposent encore de beaux jours devant eux.

330. Conclusion de la section. L'émergence d'une réglementation concurrentielle des données nécessite l'ouverture des données. Pour ce faire, l'Union européenne adopte une approche globale d'ouverture et de partage des données. Il s'agit de développer un modèle alternatif aux géants du numérique : un modèle de partage de confiance des données. Le manque de confiance est partagé entre les utilisateurs et les détenteurs de données. Ainsi, la création d'une gouvernance et d'un écosystème de confiance permettrait l'ouverture des données. Le règlement sur les données sert de fondation à la création de cet écosystème de confiance. En réalité, il s'agit d'élaborer un modèle antagoniste au modèle des géants du numérique.

Pour autant, la création d'un écosystème de confiance est un objectif chimérique. Les géants du numérique se sont développés dans l'opacité et le non-respect des droits des utilisateurs. Tant que les administrations ne disposeront pas des moyens financiers et techniques pour ouvrir leurs données, le mouvement d'ouverture demeurera une utopie. Au final, l'ouverture des données

profite aux géants du numérique qui disposent des technologies pour les exploiter, contrairement aux entreprises européennes.

Par ailleurs, l'ouverture excessive des données entraîne des risques pour les utilisateurs. L'Union européenne souhaite être pionnière dans le développement de l'intelligence artificielle. Malheureusement, la course à l'innovation de l'Union européenne rend chimérique la protection des données à caractère personnel des utilisateurs. Les principes protecteurs du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données sont écartés au nom de l'innovation. Pourtant, les objectifs économiques ne devraient pas primer sur les droits fondamentaux des individus.

331. Conclusion du chapitre. À la suite du bilan décevant du règlement de 2018 sur le libre flux des données à caractère non personnel, l'Union européenne a réitéré et consolidé sa stratégie d'ouverture des données. Il s'agit d'ouvrir les données, qu'elles soient protégées ou non, afin de développer l'innovation. Pour cela, le législateur européen va lutter contre l'accumulation massive des données en ciblant directement les géants du numérique et affirmer sa volonté d'ouvrir les données par une approche globale.

Afin de contrer la détention monopolistique des données par les géants du numérique, le règlement sur les marchés numériques met en place une régulation ciblée contre l'accès asymétrique des données. En effet, il était nécessaire de compléter le droit de la concurrence pour faire face au pouvoir de marché des données de ces acteurs. La célérité et l'opacité de leurs pratiques ont permis aux géants du numérique de détenir une masse monopolistique des données. Face à cette possession inéquitable, le règlement sur les marchés numériques qualifie ces acteurs de contrôleurs d'accès et leur interdit de combiner et de croiser les données à

caractère personnel des utilisateurs. Les pratiques de combinaison et de croisement renforcent leur pouvoir de marché et ne permettent pas une concurrence loyale. Par ailleurs, le règlement sur les services numériques adapte la qualification d'hébergeur dans le dessein de prendre en compte le rôle réel des géants du numérique. La création de la catégorie de « très grande plateforme » oblige ces acteurs à respecter des obligations proportionnelles à leur rôle sur l'environnement numérique. L'interdiction des interfaces trompeuses ou encore des contenus illicites sont des interdictions adaptées à leurs pratiques. Désormais, les géants du numérique font donc l'objet d'une régulation ciblée pour lutter contre leur accumulation massive des données.

Une fois la détention monopolistique des données réglementée, il s'agit désormais de concrétiser l'ouverture des données. Pour ce faire, l'Union européenne met en place une réglementation globale pour favoriser la disponibilité des données. Afin de libérer le flux des données et de développer l'intelligence artificielle, l'Union européenne entend élaborer un modèle disruptif de partage des données. Le partage doit se faire dans un cadre de confiance grâce à des intermédiaires de confiance. Lorsque la confiance sera acquise au sein de ce nouvel écosystème, la création d'une intelligence artificielle de confiance pourra se développer.

Pour autant, il n'existe plus d'équilibre entre l'ouverture des données et la protection des données. À ce jour, l'Union européenne souhaite être pionnière dans le développement des systèmes d'intelligence artificielle. Néanmoins, la priorisation du potentiel économique des données sur leur protection entraîne une altération progressive des principes érigés par le RGPD. Les risques pour les individus sont nombreux et les pratiques des géants du numérique sont opaques. Il faudra veiller à ne pas adapter les principes de protection au nom de l'innovation. Par ailleurs, le respect du climat doit également devenir une priorité pour l'Union européenne et les États membres, au-delà des déclarations. Plutôt que les intérêts économiques, le respect du climat et des individus doivent être prééminents à la course à l'innovation.

332. Conclusion du titre. La construction du marché unique numérique et du marché unique des données entraîne l'émergence d'une excessive diversité des normes. En effet, lors de la création du marché unique numérique, la prise en compte d'intérêts et d'objectifs antagonistes a pour conséquence la construction d'un régime transversal et complexe. L'influence des acteurs - censés être régulés - dans l'élaboration des normes ne permet pas d'établir un régime cohérent. Principalement, le régime de protection des données à caractère personnel apparaît superficiel. La distinction entre données à caractère personnel et données à caractère non personnel est poreuse et entraîne des régimes antagonistes. De surcroît, l'étude de ce régime met en exergue les limites techniques de certains droits promus par le règlement sur la protection des données à caractère personnel. Par ailleurs, la promotion de l'ouverture excessive des données entrave la protection mise en place par le règlement sur la protection des données à caractère personnel.

En effet, face au bilan décevant de l'ouverture des données à caractère non personnel, l'Union européenne a réitéré et consolidé sa stratégie de partage des données. Dans un premier temps,

l'Union européenne a mis en place une réglementation ciblée pour les acteurs du numérique. Les contrôleurs d'accès ne pourront plus combiner ou croiser les données à caractère personnel des utilisateurs afin de renforcer leur pouvoir de marché. Il s'agit de limiter le pouvoir monopolistique de ces acteurs sur les données. Une fois les pratiques des géants du numérique régulées, l'Union européenne a souhaité mettre en place une réglementation globale. Pour ce faire, les utilisateurs ainsi que les détenteurs de données doivent rétablir la confiance dans le partage de données. Autrement dit, les données ne doivent plus être détenues par certaines entreprises mais partagées dans un cadre de confiance afin de libérer les flux et de promouvoir l'innovation.

En réalité, l'application laborieuse du règlement de 2018 et l'adaptation des principes du règlement sur la protection des données à caractère personnel au nom de l'innovation démontre l'excessive diversité des normes. Il faut veiller à maintenir - voire établir - une réelle priorité sur la protection des données et le respect du climat et non sur l'économie potentielle des données. L'influence des acteurs censés être régulés dans l'élaboration des normes ainsi que leurs pratiques opaques ne permettent pas de régir un cadre cohérent. Les normes se succèdent sans réelle application concrète. De surcroît, la volonté de l'Union européenne de prioriser l'innovation sur la protection va à nouveau servir les intérêts de ces acteurs. Grâce à la masse de données qu'ils détiennent et leur puissance technologique, ils détiendront toujours l'avance nécessaire à leur développement exclusif. Le cadre normatif actuel ne permet pas de contrer la puissance de ces acteurs. Pour les entreprises européennes, la compréhension du cadre normatif actuel peut constituer une entrave à leur développement.

333. Conclusion de la partie. L'identification du cadre normatif a permis d'instaurer une typologie des différentes notions de données, typologie évolutive en fonction des pratiques et des technologies émergentes. Les notions de données à caractère personnel sont définies de manière large afin de protéger *a priori* les individus sur l'exploitation de leurs données. Pour les données à caractère non personnel, il s'agit d'une définition par opposition, afin de développer le mouvement d'ouverture des données.

En réalité, la typologie est instable au regard de l'évolution des technologies. L'usage des technologies émergentes entraîne des risques de confusions entre les notions et des risques de chevauchement. Les systèmes d'intelligence artificielle ne classifient pas les notions et font usage de l'ensemble des données. Avec le phénomène de *Big Data* et les outils d'analyse de plus en plus précis, les risques de réidentification sont prégnants et présentent des risques pour les individus.

En tout état de cause, les différentes notions de données engendrent des régimes opposés : un régime protecteur pour les données à caractère personnel et un régime d'ouverture pour les données à caractère non personnel. L'antagonisme de ces régimes a entraîné une excessive diversité des normes. Les données sont au centre du marché unique numérique, stratégie européenne depuis plusieurs années.

Pour ce faire, l'Union européenne développe son cadre normatif afin d'améliorer les politiques d'ouverture de données et de réguler les pratiques des géants du numérique. En réalité, la multiplicité des normes est renforcée par les acteurs du numérique qui influencent l'élaboration des normes afin d'y intégrer leurs intérêts mercantiles ou de freiner la logique protectrice.

PARTIE 2 :

LA MISE EN ŒUVRE LACUNAIRE DU CADRE NORMATIF

« Le risque, à terme, est que le droit perde son statut de discours autonome, autosuffisant et possédant en son sein la clé de son propre royaume. Ce royaume a mis de très longs siècles à se constituer, à se construire, à justifier aux yeux de tous sa légitimité et sa nécessité. […] Tous ces éléments sont en tout cas des pièces essentielles de l'univers juridique, joints en de subtils agencements, mais nul ne peut savoir s'ils résisteront à cette véritable révolution, à ce travail de retranscription du droit dans la forme du code. De-ci, de-là, on s'inquiète, et on cherche à se rassurer : ce monde et cette histoire ne peuvent pas mourir si vite, se rassure-t-on. Et la mythologie du « progrès » veille à bien rappeler à chacun qu'il ne sert à rien de jouer les Cassandre, et que « le meilleur des mondes » est à portée de main. Qu'il nous soit permis, tout au moins, et avec prudence, d'en douter[942]*. »*

334. Annonce de plan. L'identification du cadre normatif permet de soulever les lacunes inhérentes à la structure actuelle du cadre normatif. Tout d'abord, il s'agira de confronter le modèle pyramidal, souvent perçu comme archaïque dans le domaine du droit des données, au modèle en réseau, qui propose une approche plus subversive et décentralisée de la régulation (**Titre 1**). La difficile mise en œuvre du cadre normatif a également pour conséquence une effectivité limitée, tant au regard de la mise en œuvre des règles que de l'application des sanctions (**Titre 2**).

[942] Prevost Jean-Baptiste, « La fabrique des données : à propos du codage numérique du droit et de ses limites », Gazette du Palais, 2019, n° 3, pp. 81-86.

TITRE 1 : L'ARTICULATION ARTIFICIELLE DES NORMES

« Les situations de conflit entre normes d'ordres juridiques différents sont concrètement fréquentes, techniquement complexes, théoriquement paradoxales et politiquement sensibles. Le développement des relations internationales et, surtout, celui du droit européen ont obligé à repenser les règles classiques d'articulation des normes[943]. »

335. Notion d'articulation. L'articulation des normes est une étape fondamentale pour la mise en œuvre du cadre normatif. La notion d'articulation est une forme d'organisation, de liaison entre différentes sources. En droit, l'articulation des normes renvoie à une certaine hiérarchie normative[944]. À ce sujet, Hans Kelsen avait développé une théorie « pure » du droit, c'est-à-dire un droit épuré de toute considération politique, sociologique ou idéologique[945]. De la théorie des normes résulte la célèbre pyramide des normes, selon laquelle la conformité d'une norme dépend de la norme supérieure. L'image de la pyramide est une image rassurante, laissant transparaître un système ordonné et cohérent.

336. Inflation législative. En réalité, la théorie pure du droit est mise à mal par les faits et plus particulièrement, par l'essor du numérique. Lorsqu'on observe le droit des données, ce dernier est inexorablement issu des faits, de l'économie ou encore de la sociologie. La complexification du monde, l'accélération du progrès technique ou encore la dispersion des producteurs du contenu des normes sont autant d'éléments à prendre en compte. L'incontestable inflation législative sur le sujet des données décrédibilise l'image de la pyramide, c'est-à-dire l'image d'un système juridique ordonné et vertical. Les géants du numérique profitent de ce

[943] Deumier Pascale, *Introduction générale au droit*, éd. LGDJ, 2023, p. 291.
[944] Dictionnaire Larousse, v° « Articulation ».
[945] v. Kelsen Hans, *Théorie pure du droit*, éd. LGDJ, 1999.

basculement pour influencer artificiellement les normes. L'artificiel relève de ce « qui est le produit de l'activité, de l'habileté humaine », ou encore « qui est produit par le travail de l'homme[946] ». En effet, les acteurs du numérique profitent de la multiplicité et font en sorte de complexifier artificiellement le cadre normatif. Plus la construction est nébuleuse, plus l'articulation des normes est périlleuse et plus leurs pratiques peuvent prospérer.

337. Annonce de plan. Ainsi, il existe désormais pléthore de foyers de création de droit, aboutissant à un réseau de normes et déstabilisant l'image hiérarchique de la pyramide. À l'étude, le modèle pyramidal et hiérarchique pour le droit des données paraît archaïque (**Chapitre 1**). En l'absence de hiérarchie verticale et structurée, l'articulation d'un réseau de normes est une vision subversive, influencée par les acteurs du numérique (**Chapitre 2**).

[946] Dictionnaire Larousse, v° « Artificiel ».

Chapitre 1 : Le modèle pyramidal pour le droit des données : une vision archaïque

338. Pyramide des normes. Théoriquement, le système pyramidal est un ordre descendant dans lequel les différentes sources tiennent leur habilitation d'une norme d'un niveau supérieur pour édicter des règles. Toutes les normes sont subordonnées les unes aux autres, et s'agencent dans une logique hiérarchique, rendant le système cohérent et structuré[947]. La pyramide des normes est un circuit fermé, chaque norme respectant la procédure instituée par la norme supérieure[948]. En réalité, le système pyramidal fermé et structuré devient archaïque avec le développement du numérique. Il n'est plus question de pyramide avec une hiérarchie mais de réseau conditionné par des interactions, pouvant comporter ou non des hiérarchies[949].

339. Prééminence de l'Union européenne. En effet, avec l'essor du numérique et l'importance croissante des données, les règlements européens n'ont cessé de se multiplier. Pour les données à caractère personnel et les données à caractère non personnel, l'Union européenne est la source principale de création des normes. La prééminence de l'Union européenne dans l'élaboration des normes met à mal la logique hiérarchique reposant sur la supériorité du droit étatique (**Section 1**).

340. Diversité des foyers de création du droit. Par ailleurs, les foyers de création du droit se sont diversifiés afin de s'adapter aux technologies émergentes. Les autorités administratives indépendantes sont à l'origine d'un véritable droit de la régulation : ce dernier s'avère plus adaptable et adapté au caractère instable du numérique. L'essor de la législation déléguée démontre également les limites de la logique hiérarchique (**Section 2**).

947 Kelsen Hans, *Théorie pure du droit*, 2è édition, éd. Dalloz, 1962, p. 266.
948 Barraud Boris, *Repenser la pyramide des normes à l'ère des réseaux*, éd. Harmattan, 2012, p. 21.
949 Delmas-Marty Mireille, *Le Pluralisme ordonné. Les forces imaginantes du droit (II),* éd. Le Seuil, 2006, p. 203 ; *Ost François et Van de Kerchove, De la pyramide au réseau ? Pour une théorie dialectique du droit,* éd. FUSL, 2022.

Section 1 : Les limites de la logique hiérarchique pour le droit des données

341. Diversité des foyers de création de droit. L'élaboration du droit des données ne pouvait être confinée aux seules frontières nationales. L'absence de frontières pour les flux de données et la nationalité des grands acteurs du numérique ont nécessité une réponse européenne. Depuis plusieurs décennies, le droit des données est un droit principalement européen (I). Par-delà la prééminence du droit européen, les sources se sont diversifiées afin d'être plus malléables aux évolutions technologiques. Il existe également un phénomène d'intégration de groupes privés à l'élaboration des normes. L'européanisation du droit des données ainsi que l'intégration des groupes privés fragilisent le système de hiérarchie des normes. De surcroît, cette privatisation peut s'avérer dangereuse pour la cohérence des normes (II).

I. L'indispensable européanisation du droit des données

342. Environnement numérique. L'élaboration des normes au sujet des données devait être principalement européenne au regard de l'environnement numérique (A), rendant inévitable la marginalisation de l'État pour cette mission (B).

A) L'hégémonie nécessaire du droit européen pour l'élaboration des normes

343. Primauté et européanisation du droit des données. L'hégémonie du droit européen se traduit tout d'abord par le principe de primauté du droit communautaire (1) et plus particulièrement, par l'européanisation du droit des données (2).

1. Le principe de primauté du droit communautaire

344. Consécration du principe de primauté. Pour l'articulation entre le droit communautaire et le droit des États membres, le traité instituant la Communauté européenne du 25 mars 1957 est resté silencieux. Toutefois, la jurisprudence de la Cour européenne a rapidement consacré le principe de primauté du droit communautaire par le célèbre arrêt « Costa c/ Enel » du 15 juillet 1962[950]. En effet, la Cour va préciser la spécificité du droit communautaire par rapport au droit international en retenant : « qu'à la différence des traités internationaux ordinaires, le

[950] Cour de Justice des Communautés européennes (CJCE), aff. 6/64, Costa c/ Enel, 25 mars 1957 ; Dubouis Louis et Gueydan Claude, *Les grands textes du droit de l'Union européenne,* éd. Dalloz, 8ème édition, 2010.

traité de la CEE a institué un ordre juridique propre, intégré au système juridique des États membres lors de l'entrée en vigueur du traité et qui s'impose à leurs juridictions[951] ». La Cour ne va pas employer le terme de primauté mais évoque toutefois la « prééminence[952] » du droit communautaire[953]. C'est en 1978, grâce à l'arrêt dit « Simmenthal[954] », que la Cour consacre pour la première fois « le principe de primauté du droit communautaire[955] ». Ainsi, le droit communautaire devient partie intégrante du droit des États membres avec un rang de priorité. La primauté du droit communautaire apparaît comme cohérente au regard des objectifs de création d'un marché commun. L'application uniforme du droit communautaire était une condition nécessaire afin de développer un marché commun pour tous les États membres. Pour ce faire, le droit de l'Union européenne prime sur le droit national et la primauté de ce droit permet de garantir une application uniforme dans l'ensemble des États membres.

345. Les normes européennes. Afin de développer le marché commun, l'Union européenne dispose d'un pouvoir d'édiction des normes[956], avec un panel d'instruments juridiques trouvant leur fondement au sein de l'article 288 du TFUE[957]. Principalement, le droit dérivé est constitué de règlements et de directives. En tout état de cause, le rayonnement européen permet d'atteindre un large éventail de sujets de droit afin de garantir *a priori* une certaine cohérence

951 *Ibid.*, motifs de l'arrêt, p. 1158.

952 *Ibid.*, p. 1159 : « Attendu que la prééminence du droit communautaire est confirmée par l'article 189 aux termes duquel les règlements ont valeur " obligatoire " et sont directement applicables dans tout état membre. » ; Martucci Francesco, *Droit de l'Union européenne,* 2ème édition, éd. Dalloz, 2019.

953 Olson Terry et Cassia Paul, *Le droit international, le droit européen et la hiérarchie des normes,* éd. PUF, 2006.

954 Cour de Justice de la Communauté européenne, aff. 106/77, 9 mars 1978.

955 *Ibid.*, point 17 : « En vertu du principe de la primauté du droit communautaire , les dispositions du traite et les actes des institutions directement applicables ont pour effet , dans leurs rapports avec le droit interne des états membres , non seulement de rendre inapplicable de plein droit , du fait même de leur entrée en vigueur , toute disposition contraire de la législation nationale existante , mais encore - en tant que ces dispositions et actes font partie intégrante , avec rang de priorité , de l'ordre juridique applicable sur le territoire de chacun des états membres - d'empêcher la formation valable de nouveaux actes législatifs nationaux dans la mesure où ils seraient incompatibles avec des normes communautaires. ».

956 Picod Fabrice, « Le droit de l'Union européenne est-il soluble dans la summa divisio droit privé-droit public ? », *in* Bonnet Baptiste et Deumier Pascale (dir.), *De l'intérêt de la summa divisio droit public droit privé ?*, éd. Dalloz, 2010.

957 Traité sur le fonctionnement de l'Union européenne, article 288 : « Le règlement a une portée générale. Il est obligatoire dans tous ses éléments et il est directement applicable dans tout État membre. La directive lie tout État membre destinataire quant au résultat à atteindre, tout en laissant aux instances nationales la compétence quant à la forme et aux moyens. La décision est obligatoire dans tous ses éléments pour les destinataires qu'elle désigne. Les recommandations et avis ne lient pas. ».

au sein du territoire[958]. L'Union européenne pérennise ce mouvement d'édiction de normes avec la construction du marché unique numérique et particulièrement, du marché des données.

2. L'européanisation du droit des données

346. Activisme législatif. Afin d'encadrer la protection des données à caractère personnel et l'ouverture des données à caractère non personnel, l'Union européenne a fait l'objet d'un véritable « activisme législatif[959] ». L'Union européenne a décidé de défendre ses valeurs et de protéger les citoyens européens[960] : il s'agit du « réveil géopolitique de l'Europe » pour faire face au modèle américain et au capitalisme de surveillance[961]. L'Union a la capacité d'imposer ses règles au regard de l'importance de son marché intérieur et les plateformes du numérique ne peuvent pas se priver du marché européen pour l'exploitation des données. Pour élaborer sa politique européenne, le règlement devient l'instrument normatif privilégié de l'Union européenne[962]. Le règlement permet d'atteindre un large éventail de sujets de droit et surtout, est d'application immédiate dans tous les États membres. L'immédiateté et l'effectivité sont des déclinaisons du principe de primauté du droit communautaire[963]. Ainsi, l'Union européenne légifère activement par voie de règlements pour encadrer la protection et l'ouverture des données.

347. Européanisation du droit des données. Souvent précédé d'actes de droit souple, le droit applicable est principalement d'origine européenne pour les données à caractère personnel et les données à caractère non personnel. Néanmoins, la France a été pionnière dans certains domaines, par exemple avec l'entrée en vigueur de la Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés précédant la 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.

---

958 Bergé Jean-Sylvestre, « La summa divisio droit privé - droit public et le droit de l'Union européenne : une question pour qui ? une question pour quoi ? », *in* Bonnet Bapstiste et Deumier Pascale (dir.), *De l'intérêt de la summa divisio Droit public - Droit privé ?,* éd. Dalloz, 2010, p. 50.

959 Bertrand Brunessen, « L'émergence d'une politique européenne "spontanée" du numérique », *in* Bertrand Brunessen (dir.), *La politique européenne du numérique*, éd. Bruylant, 2023, p. 33.

960 Toledano Joëlle, « La Commission européenne, la norme et sa puissance », Pouvoirs, 185, Le Seuil, 2023.

961 Iliopoulou-Penot Anastasia, « La Constitution numérique européenne », RFDA, 2023, 945.

962 Louvaris Antoine, « Régulation économique et inflation normative », RDP, 2014, p. 304 évoquant « une irrésistible montée en puissance d'un législateur européen ».

963 Bergé Jean-Sylvestre et Robin Olivier, *Introduction au droit européen*, éd. PUF, 2008.

En revanche, la France doit se conformer à la législation européenne lorsqu'une directive ou un règlement entre en vigueur. La régulation européenne permet d'avoir *a priori* la même norme applicable sur l'ensemble du territoire de l'Union européenne, gage de sécurité juridique[964]. La primauté du droit de l'Union européenne se confirme par l'adaptabilité du droit national au droit européen. À ce jour, l'hégémonie du droit de l'Union européenne dans le droit des données est incontestable.

Le caractère de plus en plus directif des actes et la profusion des instruments a inévitablement réduit la place - auparavant hégémonique - de l'État pour l'élaboration des normes.

B) La marginalisation inévitable de l'État pour l'élaboration des normes

348. Enjeux extraterritoriaux. Les enjeux extraterritoriaux des données ne permettent plus à l'État de conserver sa place hégémonique au sein de la pyramide des normes. L'inflexion de l'État pour l'élaboration des normes (1) est confirmée par une délégation de plus en plus prégnante (2).

1. L'inflexion de la place de l'État

349. Inflexion de l'État. Au sein de la théorie de la pyramide des normes, le législateur est omniscient en détenant le monopole d'édiction des normes. Il s'agissait d'un espace normatif « fermé », épuré de toutes considérations extérieures. Avec l'arrivée d'Internet et des nouveaux usages numériques, l'inflexion de l'État était inévitable. Les données sont des objets complexes tenant à l'absence de frontière, leur dématérialisation ou encore leur technicité[965]. Au regard de cette complexité, le législateur a adapté ses outils à de nouveaux instruments tels que le droit souple ou encore le droit négocié[966]. L'État a été contraint de prendre en compte l'existence d'autres acteurs afin d'élaborer un processus d'élaboration collectif de la législation[967]. Il

964 Louvaris Antoine, « Droits fondamentaux et innovation : quelle régulation à l'ère numérique ? », Les nouveaux cahiers du Conseil constitutionnel, n° 52, p. 7.

965 Zolynski Célia, « Questions de légistique soulevées par la construction de la norme à l'aune du renouvellement des sources du droit », *in* Martine Behar-Touchais, Martial-Braz Nathalie et Riffard Jean-Francois (dir.), *Les mutations de la Norme : Renouvellement des sources du droit*, éd. Economica, 2011, p. 51.

966 Sintez Cyril, *Le droit construit*. *Penser le droit par le constructivisme*, éd. Dalloz, 2022, p. 51.

967 Chevallier Jacques, « La gouvernance, un nouveau paradigme étatique ? », Revue française d'administration publique, 105-106, Institut national du service public, 2003, p. 207.

devient un « arbitre du jeu social » s'efforçant continuellement de trouver un équilibre d'ensemble[968]. Dans le domaine des données, l'équilibre est à trouver entre la nécessité de protection des individus et le développement de l'innovation. Pour ce faire, le gouvernement n'est plus qu'un pôle d'un nouveau système de gouvernance[969] et l'État semble réduit à une intervention minimale afin d'adapter le cadre existant aux nouvelles spécificités[970]. Par conséquent, le pouvoir circule dans divers foyers de création des normes qui se développent de façon décentralisée[971].

350. Caractère décentralisé d'Internet. Le caractère décentralisé d'Internet ne permet plus au législateur de détenir le monopole d'édiction des normes[972] : l'architecture technique entraîne une décentralisation du pouvoir normatif[973] et le temps législatif n'est plus adapté aux spécificités d'Internet. Face aux enjeux du numérique, les États ont eu une prise de conscience de leur incapacité individuelle à exister et défendre leurs valeurs[974]. À ce jour, le numérique a changé de modèle « en suppléant celui de hiérarchie et de monisme par celui du réseau et du pluriel[975] ». Pour l'environnement numérique, le droit instantané et le droit souple sont plus adéquats[976]. Avec l'intervention des autorités administratives indépendantes et la présence d'acteurs privés, l'État délègue - ou partage *a minima* - son pouvoir d'édictions des normes.

---

968 Chevallier Jacques, « Autorités administratives indépendantes et État de droit », Civitas Europa, vol. 37, n° 2, 2016, pp. 143-154.

969 Moreau Defarges Philippe, « Gouvernance. Une mutation du pouvoir ? », Le Débat, n° 115, 2001, p. 166 : « Le pouvoir, même si ses racines monarchiques sont vigoureuses, ne peut plus venir d'en haut. De relation unilatérale, hiérarchique, il devient un enjeu permanent. Il n'est plus quelque chose que l'on possède, mais qui circule. Celui qui le saisit n'ignore plus qu'il peut s'évader à tout instant. La parole n'est plus l'attribut des élites mais de tous. L'ordre laisse la place à la négociation. […] Gouverner cesse de s'identifier à un organe mais devient l'affaire de tous. Chacun est simultanément gouverné et gouvernant. ».

970 Brousseau Éric, « Régulation de l'Internet », Revue économique, 52, Presses de Sciences Po, 2001.

971 Terré François et Molfessis Nicolas, *Introduction générale au droit,* éd. Dalloz, 2020, p. 500.

972 Lasserre-Kiesow Valérie, « L'ordre des sources ou le renouvellement des sources du droit », D., 2006, 2279.

973 Maxwell Winston et Taïeb Sarah, « L'accountability, symbole d'une influence américaine sur le règlement européen des données personnelles ? », Dalloz IP/IT, 2016, 123.

974 Bertrand Brunessen, « La souveraineté numérique européenne : une "pensée en acte" ? », RTD eur., n° 249, 2021.

975 Barraud Boris, *Repenser la pyramide des normes à l'ère des réseaux,* éd. Harmattan, 2012, p. 92.

976 Jestaz Philippe, « Sources du droit, sources de droit : une cartographie », *Libres propos sur les sources du droit : mélanges en l'honneur de Philippe Jestaz*, Dalloz, 2006, p. 526.

2. La progression de la législation déléguée

351. Législation déléguée. Désormais, l'État doit partager son autorité avec d'autres acteurs associés au processus décisionnels. Il cherche à associer les différents intérêts afin de prendre acte de la complexité du réel[977]. Néanmoins, la multiplication des foyers de création du droit fait apparaître un certain désordre au sein de la prétendue hiérarchie des normes[978] : l'État ne détient plus son monopole d'édiction des normes, le droit de l'Union européenne détient une place prééminente et d'autres sources gravitent autour afin d'influencer ou d'élaborer les normes[979]. D'aucuns ont estimé que la multiplication de ces foyers constitue désormais des « hiérarchies discontinues[980] » ou encore des « hiérarchies enchevêtrées[981] ». Pour autant, l'importance du droit de l'Union européenne et la marginalisation de l'État se justifient amplement au regard des caractères des données. En effet, la hiérarchie est bouleversée, pour autant ce changement était nécessaire pour ce nouvel environnement vivant. La délégation de l'élaboration de la norme à d'autres autorités se légitime généralement par la nécessité de compléter la loi afin de l'adapter aux faits[982]. En revanche, le législateur accepte une privatisation des normes pouvant s'avérer dangereuse.

II. La privatisation subreptice du droit des données

352. Construction du droit des données. Pour la construction du droit des données, le législateur a accepté la participation de groupes privés (A). Néanmoins, cette participation laisse entrevoir une privatisation du droit des données, aboutissant à un réseau de normes complexe et à la cohérence fragile (B).

---

977 Chevallier Jacques, « La gouvernance, un nouveau paradigme étatique ? », Revue française d'administration publique, Institut national du service public, 2003, p. 208 : « Leur essor témoigne du fait que les États sont désormais placés dans un contexte d'interdépendance structurelle, qui rend caduque la conception traditionnelle de la souveraineté : l'État ne dispose plus de cette puissance suprême, de cette autorité sans partage, qui étaient censées être les siennes ; il est tenu de composer avec d'autres acteurs et de se plier aux contraintes d'un cadre de coopération qui le dépasse. ».

978 Van De Kervoche Michel et Ost François, *Le système juridique entre ordre et désordre*, éd. Presses universitaires de France, 1988.

979 Lasserre Valérie, *Le nouvel ordre juridique. Le droit de la gouvernance,* éd. LexisNexis, 2015, p. 4.

980 Mireille Delmas-Marty, *Pour un droit commun*, éd. Le Seuil, 1994, p. 92.

981 Van De Kerchove Michel et Ost François, *De la pyramide au réseau ?*, éd. Facultés universitaires Saint-Louis, 2010.

982 Zolynski Célia, *op. cit*., p. 55.

A) La construction participative des normes

353. Intégration d'une source contemporaine. L'intégration du foyer contemporain privé de production du droit est une réalité (1), confirmant l'intégration d'un droit global dans la hiérarchie des normes (2).

1. La participation des organismes privés

354. Bénéfices de la participation des groupes privés. Grâce à la complexité de l'environnement numérique, les groupes privés - c'est-à-dire les entreprises du numérique - détiennent une place centrale dans l'élaboration des normes[983]. L'association de l'ensemble des acteurs, privés et publics, dans l'élaboration des normes encouragerait le respect de la réglementation[984]. En effet, la participation des groupes privés est particulièrement admise dans les secteurs marqués par des mutations technologiques et économiques extrêmement rapides[985]. L'architecture technique de l'environnement numérique nécessite la collaboration de l'ensemble des acteurs. Cette architecture a un effet ambivalent : elle peut soit être la source de nouveaux problèmes juridiques, soit être la solution afin de les prévenir voire les supprimer[986]. La participation des groupes privés permettrait de construire des normes flexibles, adaptées et constituerait une « une dynamique vertueuse[987] ». Il serait alors bénéfique de les faire participer afin d'élaborer des normes les plus idoines à leurs pratiques. L'élaboration de la norme deviendrait même attractive pour ces groupes privés[988].

---

983 Barraud Boris, « Les nouveaux défis de la recherche sur les sources du droit », Revue de la Recherche Juridique, Droit prospectif, 2017, 164, pp. 1499-1535.

984 Conseil d'État, « Internet et les réseaux numériques », Paris, 1998, p. 214 et s.

985 Norodom Anne-Thida, « La gouvernance de l'Internet », *in* Cassella Sarah, Lasserre Valérie et Lecourt Benoît (dir.), *Le droit souple démasqué : articulation des normes privées, publiques et internationales,* éd. Pedone, 2018, p. 79 : « […] parce qu'il s'agit d'un objet relativement récent ; d'un objet technique, en constante évolution, qui nécessite un droit rapidement adaptable ou parce qu'il accorde une place particulière aux acteurs privés ».

986 Gola Romain, « Le règlement européen sur les données personnelles, une opportunité pour les entreprises au-delà de la contrainte de conformité », Légicom, 2017, 29.

987 Fricero Natalie, « Algorithmes et nouvelle génération de droits humains. À propos de la Charte éthique européenne d'utilisation de l'intelligence artificielle dans les systèmes judiciaires et leur environnement », JCP, 2018, 1331.

988 Émeric Nicolas, *Penser les flux normatifs*, éd. Mare et Martin, 2018, p. 308 : « Et pour ne pas perdre la face dans la "guerre des normes", les producteurs officiels et traditionnels de la normativité juridique dans l'État de droit proposent, délèguent ou négocient auprès des grandes puissances économiques l'élaboration de cadres normatifs attractifs, compétitifs, souples et évolutifs pour une activité toujours plus fluide. ».

355. Source réelle du droit. Dans le secteur des données, la présence des groupes privés dans la construction des normes est manifeste. Il s'agit d'un phénomène contemporain dans lequel les entreprises privées prennent en charge des intérêts publics afin de les incorporer dans leur fonctionnement[989]. Le législateur confie à ces acteurs une mission de régulation d'Internet et des flux de données. En réalité, cette délégation est inévitable au regard de l'environnement opaque de ces entreprises. Par exemple, l'expression de « gatekeepers », autrement dit « gardien », employée dans le Règlement (UE) 2022/1925 du Parlement européen et du Conseil du 14 septembre 2022 relatif aux marchés contestables et équitables dans le secteur numérique (règlement sur les marchés numériques) est l'illustration manifeste du rôle dévolu à ces acteurs en matière de régulation[990]. Ainsi, les entreprises privées deviennent des « sources privées de droit[991] » ou plutôt des « sources informelles[992] ». Georges Ripert se référait déjà aux « forces créatrices du droit » pour évoquer les sources qui influencent directement ou indirectement les normes[993]. Aujourd'hui, les forces créatrices du droit s'imprègnent jusqu'au code informatique.

2. L'intégration de la norme dans le code informatique

356. Intégration d'une nouvelle source. En droit, la notion de source privée n'est pas nouvelle. La théorie de la *lex mercatoria* de Berthold Goldman a démontré que certaines formes de normativité provenaient de sources privées, notamment à travers les contrats, les usages, voire le pouvoir institutionnel d'organismes privés[994]. Le secteur du numérique est un secteur particulièrement expédient pour le développement du pouvoir de certaines entreprises dans l'élaboration de la loi[995]. Une *lex electronica* serait produite par les acteurs du numérique avec les normes techniques de l'Internet. Par ailleurs, il est possible de citer la « Netiquette », un

[989] Auby Jean-Bernard, « Les défis auxquels sont confrontés nos droits administratifs », RFDA, 2024, 241.
[990] Bismuth Régis, « L'intervention régulatrice de l'État sur les flux transfrontières circulant via Internet : Un système de contraintes », *in* Frison-Roche Marie-Anne (dir.), *Internet, espace d'interrégulation*, éd. Dalloz, 2016, p.129.
[991] Thibierge Catherine, « Le droit souple. Réflexion sur les textures du droit », RTD Civ., 2003, p. 599 ; Sintez Cyril, *Le droit construit. Penser le droit par le constructivisme,* éd. Dalloz, 2022, p. 16.
[992] Norodom Anne-Thida, *op. cit*.
[993] Georges Ripert, *Les forces créatrices du droit*, éd. LGDJ, 1955, p. 80.
[994] Goldman Berthold, « Frontières du droit et lex mercatoria », Archives de philosophie du droit, 1964, pp. 177-192.
[995] Latty Franck, « La diversité des sources du droit de l'Internet », *in* Société Française du droit international (SFDI) (dir.), *Internet et le droit international*, éd. Peton, 2014, p. 9.

ensemble de règles de comportement pour les acteurs du réseau[996] : il s'agirait d'un « contrat social » pour Internet. Avec l'essor de la régulation, les acteurs privés détiennent un pouvoir dans l'édiction des normes concernant leurs pratiques[997]. En effet, les entreprises privées ont peu à peu investi des domaines qui relevaient auparavant des pouvoirs régaliens[998]. Par exemple, certaines normes édictées dans le domaine privé peuvent devenir des normes de « droit dur » lorsque le législateur leur confère force de loi[999]. Il s'agit du passage d'un droit imposé à un « droit consenti[1000] ». Ainsi, le pouvoir normatif du législateur recule pour s'en remettre aux opérateurs économiques privés[1001]. Pourtant, il ne faut pas s'éloigner de la réalité selon laquelle les entreprises privées souhaitent une régulation des plus souples afin de pérenniser leurs pratiques[1002].

357. Intégration de la norme dans le code informatique. Concernant leurs pratiques, elles sont majoritairement centrées sur l'élaboration et la sophistication des algorithmes. Les algorithmes reposent sur des normes technologiques intégrées dans leur conception, qui n'ont pas forcément comme priorité la protection des droits fondamentaux. Avec l'émergence des systèmes d'intelligence artificielle et particulièrement des pratiques de *deep learning*, les systèmes apprennent à exécuter leurs tâches et à l'adapter grâce à l'expérience. Ils ne sont plus que de simples outils à l'aide à la décision mais prennent des décisions et effectuent des prédictions[1003] : dans ce cas, les systèmes exercent des pouvoirs normatifs[1004]. À titre d'illustration, il est d'usage pour les géants du numérique d'utiliser des algorithmes pour identifier les discours de haine sur les réseaux sociaux. La suppression du contenu relève de la capacité de l'intelligence artificielle à définir et à décider ce qu'il convient de considérer comme

---

996 La première « Netiquette » a été rédigée par Sally Hambridge en 1995, une employée d'Intel et s'intitule la « RFC 1855 », disponible sur https://datatracker.ietf.org/doc/html/rfc1855.

997 Loiseau Grégoire, « La norme en droit du numérique : de la réglementation à la régulation », *Entre art et technique : les dynamiques du droit : mélanges en l'honneur de Pierre Sirinelli,* éd. Dalloz, 2022, p. 715.

998 Sirinelli Pierre et Prévost Stéphane, « Les maîtres de la GAFAXIE », Dalloz IP/IT, 2019, 10, p. 525.

999 Zolynski Célia, *op. cit*., p. 57.

1000 Puig Pascal, « Hiérarchie des normes : du système au principe », RTD civ., 2001, p. 479.

1001 Kettani Ghizlane « Quand l'algorithme écrit le droit : les conséquences de la nouvelle normativité numérique », Dalloz IP/IT, 2022, 552.

1002 Peyrou-Bartoll Sylvie, « Quelques réflexions sur les réponses institutionnelles européennes en matière d'intelligence artificielle (IA) et de robots », *in* Sylvie Peyrou-Bartoll (dir.), *Nouvelles technologies et droit européen : quel droit face à la disruption numérique ?*, éd. Mare et Martin, 2022, p. 49.

1003 Renondin de Hauteclocque Stanislas, « L'intelligence artificielle : les différents chemins de la régulation », Éthique publique. Revue internationale d'éthique sociétale et gouvernementale, 2021.

1004 De Gregorio Giovanni, « The normative Power of Artificial Intelligence », Indiana Journal of Global Legal Studies, n° 55, 2023.

tel. Dans ce cas, le droit est un langage qui s'incarne dans les lignes de code, à l'instar de l'informatique[1005]. Surtout, ce sont les objectifs économiques de ces sociétés qui s'incarnent dans le code, et par conséquent dans la vie des individus. Et plus les systèmes d'intelligence artificielle vont modérer le contenu, plus le processus sera élaboré selon leurs intérêts lucratifs.

Le code devient alors une « source de droit ». Les applications basées sur l'apprentissage profond constituent une source normative qui façonne la société algorithmique[1006]. Les technologies prennent des décisions pouvant affecter les droits fondamentaux des individus, ce qui est fortement contestable. De surcroît, l'inintelligibilité et la complexité de ces techniques rendent cette source de droit considérablement illégitime. Pire encore, certaines normes visant à protéger la liberté d'expression dans l'environnement numérique sont déléguées à la discrétion des acteurs privés.

358. Régulateur privé. En incitant les géants du numérique à établir des normes privées, certains acteurs en ont profité pour s'ériger en véritable régulateur privé. En 2020, Facebook a créé son propre « Conseil de surveillance », qualifié illégitimement de « Cour suprême »[1007]. Le Conseil a pour principale mission d'examiner les affaires complexes de suppression de contenu sur ses plateformes Facebook et Instagram « conformément aux règles de contenu et aux valeurs de Facebook[1008] ». Le Conseil pourra également se fonder sur les décisions antérieures, lesquelles « ont une valeur de précédent et devront être considérées comme très convaincantes lorsque les faits, les politiques applicables ou d'autres facteurs sont essentiellement similaires[1009] ». Sans aucun doute, une assimilation avec la jurisprudence peut être relevée. L'entité *ad hoc* sélectionnera elle-même les affaires de modération à étudier. La sélection discrétionnaire des cas interroge sur la légitimité d'un organe à juger les faits de sa propre plateforme[1010].

1005 Teller Marina, « Vers l'acceptabilité sociale des algorithmes ou comment passer de l'"algocratie" à la démocratie algorithmique », Revue pratique de la prospective et de l'innovation, n°1, 2022.
1006 De Gregoria Giovanni, *op. cit.*
1007 Heymann Jérémy, « La nature juridique de la "Cour suprême" de Facebook », *in* Frison-Roche Marie-Anne (dir.), *La juridictionnalisation de la compliance*, éd. Dalloz, 2023, p. 166 ; Benabou Valérie-Laure, « Bannir Trump de Facebook et Twitter, so what ? », Le Club des Juristes, 6 juillet 2021.
1008 Charte du Conseil de surveillance, article 2.
1009 *Ibid*., article 2 paragraphe 2 alinéa 2.
1010 G'Sell Florence, « Le Conseil de surveillance de Facebook et l'affaire Trump. Les limites du concept de "tribunal d'entreprise" », La Semaine Juridique Edition Générale n° 22, 31 mai 2021.

En effet, la portée des décisions interpelle sur la possibilité conférée au conseil de définir des standards en matière de liberté d'expression et de modération[1011]. En établissant une justice privée, Facebook fait l'objet d'une régulation obscure, centralisée et régie par une éthique contestable[1012]. La régulation privée illustre la volonté de ces acteurs d'intégrer de manière systématique la norme privée[1013]. En réalité, les géants du numérique ne sont pas légitimes à élaborer un système judiciaire privé, étant donné qu'ils ne sont pas choisis par un processus démocratique mais sont plutôt des « oligarques technologiques politiquement irresponsables [qui] exercent des pouvoirs de censure semblables à ceux d'un État[1014] ». Il est indispensable de rappeler qu'il s'agit d'acteurs non élus et non étatiques. Ainsi, cette privatisation de la régulation de la liberté d'expression en ligne interroge sur la capacité et la volonté de ces acteurs privés de modérer effectivement les contenus[1015].

359. Tempérament par le « droit dur ». Afin de rétablir *a minima* la distinction entre le pouvoir étatique et privé, le Règlement (UE) 2022/2065 du 19 octobre 2022 du Parlement européen et du Conseil relatif à un marché unique des services numériques (DSA) prévoit une obligation de transparence et de recours pour les utilisateurs. Il prévoit que les « destinataires du service devraient pouvoir contester facilement et efficacement certaines décisions des fournisseurs de plateformes en ligne, relatives à l'illicéité d'un contenu ou à son incompatibilité avec les conditions générales, qui ont une incidence négative pour eux[1016] ». En outre, les fournisseurs de plateformes en ligne doivent permettre aux utilisateurs de choisir « entre le mécanisme interne de traitement des réclamations, un règlement extrajudiciaire des litiges et la possibilité d'engager, à tout moment, une procédure juridictionnelle[1017] ». Il était indispensable

[1011] Ndior Valère, « Le Conseil de surveillance de Facebook et la protection des libertés », RDLF, n° 23, 2022.
[1012] Gaye-Palettes Matthieu, « Entre justice privée et justice étatique », Pouvoirs, 178, septembre 2021, 21.
[1013] Ndior Valère, « Le Conseil de surveillance de Facebook, "service après-vente" de la liberté d'expression ? », D., 2020, 1474 : « Si l'intention paraît louable, la perspective de voir se créer un panel de Google, un mécanisme d'inspection de Twitter ou un tribunal paritaire d'Uber, dotés de référentiels propres et d'une compétence mondiale, à l'instar du Conseil de surveillance, donne le vertige. ».
[1014] Bloch-Wehba Hannah, « Global Platform Governance : Private Power in the Shadow of the State », SMU Law Review, Volume 72, 2019.
[1015] Cluzel-Métayer Lucie, « Contrôler les contenus ? », Pouvoirs n° 185, Le Seuil, 2023.
[1016] Règlement (UE) 2022/2065 du 19 octobre 2022 du Parlement européen et du Conseil relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (règlement sur les services numériques), considérant 58.
[1017] *Ibid.*, considérant 59.

qu'un règlement tempère l'intégration d'une justice privée dans le débat d'un sujet aussi sensible pour les droits des individus et la démocratie[1018].

Ainsi, les groupes privés et les régulateurs interagissent constamment, non pas dans une logique hiérarchique mais plutôt une logique de réseau.

B) La constitution d'un réseau complexe de normes

360. Les conséquences de la diversité des sources. La multiplicité des acteurs entraîne *de facto* un réseau complexe de normes. La notion de réseau rend obsolète la pyramide des normes (1), mettant en avant un univers désormais non hiérarchique (2).

1. L'obsolescence de la pyramide des normes

361. Multiplication des foyers de droit. La multiplication des foyers de droit décrédibilise l'image d'un système juridique ordonné et vertical. La pyramide des normes serait devenue « un complexe de hiérarchies réversibles et d'accommodements délicats[1019]». À ce jour, avec la puissance et l'influence des groupes privés dans la construction des normes, la nature juridique d'une règle ne dépend plus de sa forme mais de la puissance de son auteur[1020]. Il existe des sources de droit informelles qui se trouvent dans les interstices de la pyramide[1021]. Par conséquent, le droit consenti se classerait à un rang « infra-hiérarchique[1022] ». La logique ne

[1018] Saillant Clara, « Modération en ligne à la demande de la police londonienne : le Conseil de surveillance de Meta s'improvise régulateur et juge », Dalloz Actualité, 15 décembre 2022 : « La création d'entités similaires au Conseil de surveillance de Meta devrait être accueillie positivement si cela permet, comme cela semble être le cas pour Facebook et Instagram, une meilleure application des libertés fondamentales et une plus grande transparence sur les pratiques de ces entreprises. En revanche, il ne faut pas se leurrer, la vigilance est de mise, car sans possibilité de recours devant des autorités administratives ou publiques ou des organes judiciaires étatiques, le risque d'un développement de la justice privée ne fait que commencer. ».

[1019] Vanderlinden Jacques, « Contribution en forme de mascaret à une théorie des sources du droit au départ d'une source délicieuse », RTD civ., 1995, 69.

[1020] Mongoin David, *Philosophie du droit*, éd. Dalloz, 2022, p. 304.

[1021] Mekki Mustapha, « Propos introductifs sur le droit souple », *in* Association Henri Capitant des amis de la culture juridique française (dir.), *Le droit souple*, éd. Dalloz, 2009, p. 14.

[1022] Puig Pascal, *op. cit.* : « Les incertitudes proviennent, pour l'essentiel, du pluralisme des sources de droit dont le développement perturbe le contenu de la hiérarchie des normes autant que son ordonnancement. Du sommet à la base de la pyramide tendent à s'infiltrer des normes dont la formation échappe, en tout ou partie, à la médiation étatique, remettant en cause le postulat du positivisme légaliste sur lequel est encore largement conçue la théorie contemporaine des sources du droit. ».

serait donc plus celle d'une pyramide régie par les seuls pouvoirs publics dans un système vertical mais bien une logique de dialogue entre les parties prenantes, privées et publiques, voire par une co-régulation en « réseau »[1023]. La complexité de l'environnement numérique européanisé et globalisé encourage les foyers de production de droit souple[1024].

En réalité, la multiplicité et la complexité profitent à ces sociétés privées qui ne souhaitent pas être soumises à un cadre normatif trop inflexible. Le réseau de normes leur est profitable sans clé de lecture : ils profitent de leurs pouvoirs pour participer à la construction du cadre dont ils sont les protagonistes.

2. La substitution de source par le pouvoir

362. Notion de « pouvoir ». Le système de droit n'est pas nécessairement en crise, en revanche il est en mutation. Dans le domaine du numérique et pour le droit des données, le système a dû s'adapter à ce nouvel environnement. La réponse devait être européenne pour l'élaboration des règlements d'application directe et surtout, harmonisée et uniforme. Néanmoins, l'influence des groupes privés dans la construction des normes est contestable. Certains auteurs détournent même la notion de « source » pour la notion de « pouvoir » afin d'évoquer leur influence[1025]. En effet, les entreprises privées du numérique détiennent un pouvoir d'influence, voire de manipulation, avec une domination économique inédite[1026]. Le cumul de puissance de ces acteurs leur permet de se placer au-dessus des lois nationales et de créer des risques pour l'État de droit[1027].

363. Droit global. Dans ce nouveau système, voire espace juridique, le droit global serait le nouveau « terrain de jeux d'acteurs, principalement des individus et des sociétés commerciales, disposant des capacités juridiques et financières pour choisir le meilleur ordre juridique applicable à leurs relations de droit[1028] ». Le droit global s'illustrerait par une forme extrême de

---

1023 Latty Franck, *op. cit*., p. 13.

1024 Antoine Louvaris, « Le droit souple a trouvé ses juges : un foisonnement régulé », Justice et Cassation, 2023, 191.

1025 Caire Anne-Blandine, *Les nouveaux pouvoirs. Approche pluraliste des foyers de création du droit*, éd. Bruylant, 2017.

1026 Eeckhoudt Marjorie, « Propos introductifs », Revue internationale de droit économique : Les grandes entreprises échappent-elles au droit ?, Association internationale de droit économique, 2016.

1027 Iliopoulou-Penot Anastasia, « La Constitution numérique européenne », RFDA, 2023, 945 .

1028 Sintez Cyril, *op. cit*., p. 72.

forum shopping pour ces acteurs. Les groupes privés ont tout intérêt à s'infiltrer dans l'élaboration des normes afin d'influer sur le contenu de la norme pour ensuite avoir le pouvoir sur son application. Aujourd'hui, les normes s'élaborent en réseau rendant obsolète la logique pyramidale[1029].

[1029] v. Ost François et Van de Kerchove Michel, *De la pyramide au réseau ? Pour une théorie dialectique du droit*, éd. Broché, 2022.

364. Conclusion de la section. L'environnement numérique est un espace sans frontière, dominé par des flux de données et contrôlé par de puissants acteurs privés. La complexité et l'opacité de cet environnement ont mis à mal la logique hiérarchique des normes.

Tout d'abord, la prééminence du droit de l'Union européenne fragilise la hiérarchie des normes. En réalité, face à l'absence de frontière de ce nouvel environnement, la réponse devait être nécessairement européenne. Les défis de l'encadrement des données ne pouvaient se résoudre au niveau national. Ainsi, l'activisme législatif de l'Union européenne est louable au regard de ce nouvel environnement.

De façon plus critiquable, la logique hiérarchique est tempérée par le recul du législateur sur le monopole d'édition des normes, pilier central de la logique Kelsienne. Il n'existerait plus de pyramide hiérarchique mais un réseau de normes complexes et enchevêtrées. La complexité est enrichie par la délégation du législateur de certaines problématiques à des groupes privés afin d'adapter les normes aux pratiques, ou plus précisément à leurs pratiques. La privatisation des normes participe à la fragilisation de la cohérence du cadre normatif. Les groupes privés s'imbriquent dans le processus d'élaboration des normes et agrémentent la complexité. En pratique, ils intègrent les normes privées directement dans le code informatique : le code devient une source de droit grâce à leur domination technologique.

Ainsi, la logique verticale gouvernée par l'État est substituée par une logique en réseau, aboutissant à une nouvelle gouvernance. Le dialogue est instauré entre les parties prenantes, privées et publiques, et constitue un système attrayant pour les acteurs privés. Pour les individus, l'opacité et les limites du contrôle constituent des risques pour leurs droits fondamentaux.

Section 2 : La nouvelle logique de gouvernance du droit des données

365. Notion de gouvernance. La nouvelle logique de gouvernance représente une mutation de la façon de gouverner dans laquelle les pouvoirs - qui ne sont pas tous publics - se coordonnent afin d'atteindre des consensus dans un environnement incertain et complexe[1030]. L'environnement numérique ne permet plus une prise de décision unilatérale et monopolistique de la part du législateur. Au contraire, la gouvernance est un changement de paradigme marqué par le recul du pouvoir étatique et la croyance dans l'autorégulation des groupes sociaux[1031]. Ainsi les caractéristiques de la gouvernance sont en rupture avec la logique hiérarchique de la pyramide des normes.

366. Notion de droit souple. En effet, les normes au sein de la gouvernance ne s'apparentent pas à des lois ou des règlements. Dans la logique de gouvernance, les normes s'illustrent par une grande diversité, dont le droit souple est prééminent (I). Le terme souple renvoyant à ce qui est « docile » et « qui, par sa variété, sa richesse, est susceptible de produire des effets très divers, de s'adapter aisément à des situations, à des intérêts divers[1032] ». Le droit souple permet de s'adapter aux intérêts de chacun. En réalité, ce sont les acteurs du numérique qui vont bénéficier de cette souplesse, entraînant un enchevêtrement complexe de normes dont l'articulation est difficilement saisissable. Ainsi, la frontière entre les notions de droit dur et droit souple s'avère poreuse. L'intégration excessive de « souplesse » dans les normes par les groupes privés comporte des risques (II).

1030 Lasserre Valérie « Règles privées et publiques de gouvernance », *in* Cassella Sarah, Lasserre Valérie et Lecourt Benoît (dir.), *Le droit souple démasqué : articulation des normes privées, publiques et internationales*, éd. Pedone, 2018, p. 5.

1031 Berthelet Pierre « Le droit européen de la cybersécurité à l'épreuve de la nouvelle gouvernance : réflexions autour d'une normativité réticulaire et néomoderne », *in* Sylvie Peyrou-Bartoll (dir.), *Nouvelles technologies et droit européen : quel droit face à la disruption numérique ?*, éd. Mare et Martin, 2022, p. 237 ; Chevallier Jacques, « La gouvernance, un nouveau paradigme étatique ? », Revue française d'administration publique, Institut national du service public, 2003, pp. 203-217.

1032 CNRTL, v° « Souple », disponible en ligne.

I. La prépondérance du droit souple pour la gouvernance

367. Inflation et influence du droit souple. Depuis plusieurs années, et particulièrement pour les données, le droit souple connaît une inflation vertigineuse (A). Par-delà l'inflation quantitative, le droit souple est également caractérisé par son influence décisive (B).

A) L'inflation vertigineuse du droit souple

368. Prééminence et prolifération. Afin de comprendre l'inflation vertigineuse du droit souple, il est nécessaire de revenir sur la prééminence des autorités administratives indépendantes (1). La présence de ces autorités de régulation entraîne *de facto* une prolifération d'actes de droit souple (2).

1. La prééminence des autorités administratives indépendantes pour la régulation des données

369. Absence des autorités administratives indépendantes dans la pyramide des normes. Au sein de la pyramide des normes de Kelsen, les autorités administratives indépendantes sont absentes[1033]. Pour la Professeure Martine Lombard, trouver la place des autorités administratives indépendantes dans la pyramide des normes relève de l'antinomique[1034]. Les autorités de régulation sont les protagonistes du changement de conception hiérarchique, d'une nouvelle forme de gouvernance. En effet, ces autorités vont prendre le relais du gouvernement ou de l'autorité judiciaire lorsqu'ils sont défaillants ou inappropriés pour un secteur ou un domaine particulier[1035]. Selon le domaine, les autorités administratives indépendantes peuvent être dotées d'un pouvoir d'édiction de normes, d'émission d'avis ou de recommandations. Elles peuvent également être dotées d'un pouvoir d'autorisation, d'investigation ou encore de sanction. L'expertise de ces autorités dans chaque domaine leur confère une certaine légitimité réceptionnée par les destinataires. Les destinataires des normes seraient davantage enclins à

1033 Barraud Boris, *Repenser la pyramide des normes à l'ère des réseaux*, éd. Harmattan, 2012, p. 151.
1034 Lombard Martine, « Régulation et hiérarchie des normes », *in* Lombard Martine (dir.), *Droit et économie de la régulation. Règles et pouvoirs dans les systèmes de régulation*, éd. Presses de Sciences Po, 2004.
1035 Barthez Anne-Sophie, « Les avis et recommandation des autorités administratives indépendantes », *in* Association Henri Capitant des amis de la culture juridique française, *Le droit souple*, éd. Dalloz, 2009, p. 60.

respecter des prescriptions négociées et proposées par ces autorités[1036]. Désormais, la norme opère par « persuasion » et non par « autoritarisme[1037] », confirmant l'avènement d'un droit « postmoderne[1038] ». Le droit postmoderne s'adapte logiquement à notre société transformée par la révolution numérique[1039]. Pour ce faire, la logique de réglementation se complète par une logique de régulation.

370. De la réglementation à la régulation. La réglementation vient de l'État et quand l'État se désengage par la privatisation, la régulation permet de compléter le système normatif[1040] : la régulation est plus souple et permet de s'adapter à la spécificité d'un secteur. La spécificité implique que les règles générales ne conviennent pas à tous les secteurs et aux différents objectifs[1041]. Dans les domaines régulés, les sujets sont particulièrement complexes et techniques, ne pouvant être maîtrisés exclusivement par le pouvoir politique[1042]. En droit des données, les enjeux sont évolutifs et les règles doivent faire l'objet d'une adaptation quasi permanente. Les autorités administratives indépendantes sont avant tout une adaptation des modes d'intervention et des principes d'organisation de l'État[1043]. Le régulateur aménage les principes fondamentaux et règles afin de s'adapter à la diversité des enjeux et des situations[1044]. En pratique, les diverses autorités ont des finalités différentes, c'est-à-dire la protection d'une liberté fondamentale ou encore le maintien du jeu de la concurrence. Le droit des données bouleverse cette dichotomie en intégrant des enjeux de libertés fondamentales et de concurrence. Ainsi, les autorités administratives indépendantes sont amenées à fixer des règles

1036 Loiseau Grégoire, « La norme en droit du numérique : de la réglementation à la régulation », *Entre art et technique : les dynamiques du droit : mélanges en l'honneur de Pierre Sirinelli*, éd. Dalloz, 2022, p. 66.
1037 Carbonnier Jean, *Sociologie juridique*, éd. PUF, 2004, p. 146.
1038 Jean Chevallier, « Vers un droit postmoderne ? », *in* Clam Jean et Martin Gilles (dir.), *Les transformations de la régulation juridique*, éd. LGDJ, 1998, p. 21.
1039 Louvaris Antoine, « Le droit souple a trouvé ses juges : un foisonnement régulé », Justice et cassation, 2023. 191.
1040 Raymond Martin, « Le droit en branches », D., 2002, p. 1703.
1041 Frison-Roche Marie-Anne, « L'hypothèse de l'interrégulation », *in* Frison-Roche Marie-Anne (dir.), *Les risques de la régulation*, éd. Dalloz, 2005, p. 70.
1042 Haquet Arnaud, « Le pouvoir réglementaire des autorités administratives indépendantes », RDP, 2008, p. 393.
1043 Chevallier Jacques, « Le statut des autorités administratives indépendantes : harmonisation ou diversification ? », RFDA, 2010, 896.
1044 Geffrey Edouard, « Droits fondamentaux et innovation : quelle régulation à l'ère numérique ? », Les nouveaux cahiers du Conseil Constitutionnel, n° 52, p. 7.

techniques *ex ante*, qualifiées de droit souple, afin d'accompagner les entreprises dans une relation de confiance[1045].

2. La prolifération des actes de régulation des données

371. Diversité d'appellations. Avec la célérité des technologies émergentes, les actes de droit souple se succèdent à un rythme effréné[1046]. Il s'agit d'inciter plutôt que de contraindre les acteurs du numérique, par l'usage de diverses appellations avec des degrés différents de force contraignante[1047]. Désormais, en parallèle des sources traditionnelles que sont la Constitution, les traités internationaux, les règlements ou les lois, des actes aux appellations diverses comme les recommandations, les avis, les codes de bonne conduite, les lignes directrices ou encore les livres blancs ou verts s'élaborent par des sources multiples et novatrices[1048]. À ce jour, il existe une pléiade d'appellations de normes susceptibles d'entrer en conflit : « leur volume n'égale que la variété de leurs appellations[1049] ». Toute cette diversité d'appellations de nouvelles normes complexifie la compréhension du cadre normatif[1050].

372. Absence de hiérarchie. Les différentes normes ne disposent pas de hiérarchie entre elles[1051]. La logique pyramidale selon laquelle chaque norme tire sa validité de celle qui lui est supérieure est désuète avec les nouvelles normes[1052]. Ces dernières ne peuvent être assimilées à

1045 Favro Karine, « La CNIL, une autorité à "l'âge de la maturité" », Dalloz IP/IT, 2018, p. 464.

1046 Boy Laurence, « Réflexions sur le droit de la régulation », D., 2001, 3031.

1047 Thibierge Catherine, « Le droit souple. Réflexion sur les textures du droit », RTD civ., 2003, p. 599.

1048 Terré François et Molfessis Nicolas, *op. cit.*, p. 526.

1049 Berthelet Pierre, « Le droit européen de la cybersécurité à l'épreuve de la nouvelle gouvernance : réflexions autour d'une normativité réticulaire et néomoderne », *in* Sylvie Peyrou-Bartoll (dir.), *Nouvelles technologies et droit européen : quel droit face à la disruption numérique ?*, éd. Mare et Martin, 2022, p. 242.

1050 Gaudemet Yves, « La régulation économique ou la dilution des normes », RDP, 2017, p. 23 : « On y range les nombreuses recommandations, avis, normes de référence, modèles, schémas, propositions, plans, préconisations, référentiels, feuilles de route, codes de bonne conduite ou de bonnes pratiques, chartes ou encore protocoles accords informels ou de partenariat, programmes, toutes dénominations dont la liste s'allogne presque tous les jours, à la libre inventitivité des régulateurs, qui sonnent tellement plus moderne à l'oreille que les vieux outils normatifs et dont on vante la souplesse et la concertation qu'ils affichent. ».

1051 Loiseau Grégoire, « La norme en droit du numérique : de la réglementation à la régulation », *op. cit.*, p. 314.

1052 Jestaz Philippe, « Sources du droit, sources de droit : une cartographie », *op. cit.*, p. 543: « La classification tend à s'estomper par le développement de réalités et de concepts intermédiaires. D'une part, sur le plan des sources, avec la montée en puissance des sources non formelles, qui trouvent peu à peu leur place parmi les sources de droit. D'autre part, sur le plan des normes, avec la conceptualisation du droit spontané, à l'interface du droit édicté et des sources substantielles, et avec celle du droit souple, sorte d'intermédiaire entre le droit dur et non-droit. ».

de véritables normes, même lorsqu'il s'agit de normes issues d'une délégation du législateur[1053]. Par conséquent, les nouvelles normes ne s'intègrent aucunement dans la hiérarchie classique[1054]. De surcroît, la diversité des autorités de régulations précitée va inévitablement amplifier le conflit de nouvelles normes les prochaines années.

373. Approche par le réseau. Ainsi, l'approche en réseau inspirée des auteurs François Ost et Michel Van De Kerchove permet de mieux appréhender cette complexité[1055]. Il s'agirait d'une gouvernance en réseau permettant l'élaboration de normes participatives, de nouvelles formes de régulation avec un formalisme juridique plus faible[1056]. Le passage de la logique déclarative à la logique d'*accountability* du règlement sur la protection des données à caractère personnel illustre ce changement de paradigme. Plutôt qu'une logique hiérarchique découlerait une logique de prévention afin « d'embrasser de façon effective la réalité dynamique et évolutive de l'univers numérique[1057] ». La confiance est transmise par les acteurs dits traditionnels - législatif et réglementaire - aux entreprises ou acteurs du numérique[1058] et lorsque la confiance est rompue, la logique de sanction prendrait le relais. Les acteurs du numérique auraient alors tout intérêt à respecter les règles préventives afin de ne pas succomber à la sanction. *A priori*, la gouvernance régie par le droit souple aurait une logique vertueuse ainsi qu'une influence décisive.

1053 Martial-Braz Nathalie « Propos introductifs », *in* Martial-Braz Nathalie, Riffard Jean-Francois, Béhar-Touchais Martine (dir.), *Les mutations de la norme : le renouvellement des sources du droit*, éd. Economica, 2011, p. 11.

1054 Puig Pascal, « Hiérarchie des normes : du système au principe », RTD civ., 2001, p. 479.

1055 Van De Kerchove Michel et Ost François, *op. cit*.

1056 Berthelet Pierre, *op. cit*., p. 238.

1057 Gola Romain, « Le règlement européen sur les données personnelles, une opportunité pour les entreprises au-delà de la contrainte de conformité », Légicom, 2017, 29.

1058 Falque-Pierrotin Isabelle, « L'Europe des données ou l'individu au coeur d'un système de compliance », *in* Frison-Roche Marie-Anne (dir.), *Régulation, Supervision, Compliance*, éd. Dalloz, 2017, p. 30.

B) L'influence décisive du droit souple

374. Influence sur les lois et les individus. Les nouvelles sources s'intègrent dans le réseau de normes et détiennent une influence décisive sur le droit (1) ainsi que sur les individus (2).

1. L'intégration du droit souple dans la loi

375. Foyer de droit souple. L'essor des technologies disruptives entraîne un foisonnement des actes de droit souple. Dans un premier temps, afin d'évaluer et d'appréhender les technologies émergentes, les différents organes émettent des normes de droit souple. En réalité, la démarche régulatoire anticipe la future réglementation qui est d'ores et déjà en discussion. La gouvernance permet d'établir une veille sur des événements non anticipés et non anticipables[1059]. À titre d'illustration, l'intelligence artificielle a été un foyer actif de droit souple avant l'entrée en vigueur du Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle. Plusieurs livres, recommandations ont été mis en place à titre d'essai avant le règlement définitif[1060]. L'efficacité de ces différentes normes de droit souple va ensuite être évaluée afin de savoir quelles normes peuvent être incitatives et quelles normes doivent être directrices. Il arrive parfois que les règlements intègrent directement des normes de droit souple.

376. Code de conduite. L'intégration des normes de droit souple permet une d'établir une logique de co-régulation. Le législateur établit la norme impérative et les acteurs du numérique peuvent établir des normes privées à l'appui. Dès 2016, le Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 prévoyait que les États membres, les autorités de contrôle ainsi que le comité et la Commission européenne encouragent l'élaboration de codes de conduite ou certifications, permettant la bonne application du

---

1059 Curien Nicolas, « La régulation réflexive à travers le miroir de la transition numérique », *in* Marie-Anne Frison Roche (dir.), *Internet, espace d'interrégulation*, éd. Dalloz, 2016, p. 134 : « La gouvernance ou la régulation réflexive réclament ainsi l'exercice ex ante d'une veille active et délibérée, mieux qu'une simple réaction ex post non calculée face à des évènements non anticipés. ».

1060 Pour une liste d'exemples non exhaustive : Conseil de l'Europe, « La convergence technologique, l'intelligence artificielle et les droits de l'homme », Recommandation 2102 (2017) ; Conseil de l'Europe, Recommandation sur les impacts des systèmes algorithmiques sur les droits de l'homme (CM/Rec (2020)1 ; Conseil de l'Europe, « Lignes directrices sur l'intelligence artificielle et la protection des données », 25 janvier 2019.

règlement en fonction de la spécificité de chaque acteur[1061]. Pour ce faire, des associations et organismes représentant certaines catégories de responsable de traitement vont élaborer ces codes afin de préciser les modalités d'application du règlement précité.

377. Pouvoir de contrôle. Ensuite, les autorités nationales disposent d'un pouvoir de contrôle pour vérifier la réelle application de ces codes. Lorsque les responsables de traitement s'engagent à appliquer un code de conduite, les autorités ont le pouvoir de procéder au contrôle du respect dudit code[1062]. Les acteurs du numérique ont tout intérêt à adhérer à ces codes de conduite afin d'améliorer leur réputation, entachés ces dernières années par les différents scandales sur l'utilisation des données à caractère personnel de leurs utilisateurs[1063]. Néanmoins, il est d'usage pour ces acteurs de ne pas respecter les obligations auxquelles ils se sont soumis volontairement[1064]. La promotion de la *soft law* leur est donc profitable, sans en être réellement contraint.

2. La création d'un droit souple « contraignant »

378. Code de conduite « contraignant ». Afin de pallier l'insuffisance de l'autorégulation, le Règlement (UE) 2022/2065 du 19 octobre 2022 du Parlement européen et du Conseil relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (règlement sur les services numériques) oblige désormais les très grandes plateformes à mettre en œuvre les codes de conduite auxquels elles adhèrent : la formulation démontre la pédagogie élémentaire

---

1061 Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), article 40 paragraphe 1 : « Les États membres, les autorités de contrôle, le comité et la Commission encouragent l'élaboration de codes de conduite destinés à contribuer à la bonne application du présent règlement, compte tenu de la spécificité des différents secteurs de traitement et des besoins spécifiques des micro, petites et moyennes entreprises. ».

1062 *Ibid.*, paragraphe 4 : « Le code de conduite visé au paragraphe 2 du présent article comprend les mécanismes permettant à l'organisme visé à l'article 41, paragraphe 1, de procéder au contrôle obligatoire du respect de ses dispositions par les responsables du traitement ou les sous-traitants qui s'engagent à l'appliquer, sans préjudice des missions et des pouvoirs de l'autorité de contrôle qui est compétente en vertu de l'article 55 ou 56. ».

1063 Poullet Yves, « Les modes alternatifs de régulation : codes de conduite, certifications et ADR dans le RGPD », *in* De Terwangne Cécile et Rosier Karen (dir.), *Le Règlement général sur la protection des données (RGPD / GDPR). Analyse approfondie*, éd. Larcier, 2018, pp. 613-635.

1064 Castets-Renard Céline, *Droit du marché unique numérique et intelligence artificielle*, éd. Bruylant, 2020, p. 287.

dont doit faire preuve les règlements pour ces acteurs majoritairement de mauvaise foi. En outre, le code européen contre la désinformation a été révisé et présenté le 16 juin 2022 par la Commission européenne. Les principales mesures ont trait à la publicité en ligne, à la lutte contre les pratiques de manipulation, à la transparence et enfin, à l'accès aux données. Cette fois-ci, le respect de ces engagements par les signataires sera évalué par des indicateurs communs, permettant de mesurer réellement les actions des plateformes. Le droit souple devient un indicateur pour la sanction. En réalité, ce sont les acteurs qui apprécient leurs propres risques, instaurant un dialogue entre les sociétés privées et les régulateurs, vidant de sa substance le caractère contraignant de certaines obligations. La prééminence du droit souple comporte des risques.

II. Les risques de la prééminence du droit souple

379. Risques pour la cohérence. La prééminence du droit souple pour les données entraîne des risques quant à l'incertitude de sa nature. En effet, l'intégration du droit souple dans les récents règlements trouble la frontière entre droit souple et droit dur (A). Par ailleurs, la coproduction du droit avec les groupes privés peut s'avérer préjudiciable pour la cohérence du système normatif (B).

A) L'incertaine frontière entre droit souple et droit dur

380. Recherche d'une cohérence. L'intégration du droit souple dans les règlements et la reconnaissance de la force normative de certains actes de droit souple troublent la frontière entre l'obligatoire ou non (1), ayant pour conséquence une forme de dilution de la norme dans le système (2). Afin de rétablir une certaine cohérence dans le système normatif, le juge contrôle les actes de droit souple.

1. La reconnaissance de force normative des actes de droit souple

381. Reconnaissance de la force normative. Pour prendre en compte l'« angle mort[1065] » du contrôle juridictionnel, le Conseil d'État va modifier l'objet du recours pour excès de pouvoir. Dans deux arrêts de 2016, le Conseil d'État estime que « les avis, recommandations, mises en garde et prises de position adoptés par les autorités de régulation dans l'exercice des missions dont elles sont investies, peuvent être déférés au juge de l'excès de pouvoir lorsqu'ils revêtent le caractère de dispositions générales et impératives ou lorsqu'ils énoncent des prescriptions individuelles dont ces autorités pourraient ultérieurement censurer la méconnaissance ; […] ces actes peuvent également faire l'objet d'un recours, introduit par un requérant justifiant d'un intérêt direct et certain à leur annulation, lorsqu'ils sont de nature à produire des effets notables, notamment de nature économique, ou ont pour objet d'influer de manière significative sur les comportements des personnes auxquelles ils s'adressent[1066]. ». Dans l'affaire « Gisti », le Conseil d'État précise que ces actes peuvent être des documents ayant une portée générale, qu'il s'agisse de circulaires, de notes ou de présentations[1067]. La liste n'est pas exhaustive et permet de s'adapter aux évolutions des différentes appellations. Le caractère déterminant est l'effet de droit, c'est-à-dire l'impact sur les destinataires indirects ou directs de la norme[1068]. La recevabilité du recours est donc conditionnée aux effets notables de la décision, effets notamment économiques[1069]. Pour autant, la notion d'effets « notables » tend à réduire la possibilité de reconnaître une force normative à ces actes.

382. Respect d'une certaine cohérence. L'ouverture du recours pour excès de pouvoir permet de veiller à ce que les normes produites par les autorités administratives indépendantes respectent l'ensemble des normes supérieures, afin de garantir une certaine cohérence du système[1070]. En effet, les autorités administratives ne disposent pas de la même légitimité que

---

1065 Idoux Pascale, « Le temps de la régulation », *in* ADFA (dir.), *Le temps en droit administratif*, éd. Dalloz, 2022.

1066 Conseil d'État, aff. Société Faiversta International GMBH, n° 368082, 21 mars 2016, publié au recueil Lebon ; Conseil d'État, aff. Société NC Numericable, n° 390023, points 4 et 5.

1067 Conseil d'État, aff. GISTI, n° 418142, 12 juin 2020, publié au recueil Lebon.

1068 Emeric Nicolas et Matthieu Robineau, « Prendre le droit souple au sérieux ? À propos de l'étude annuelle du Conseil d'État pour 2013 », La semaine juridique, n° 43, 2013, p. 1962.

1069 Pauliat Hélène, « La contribution du droit souple au désordre normatif », RDP, 2017, p. 59.

1070 Benezech Ludovic, « Les actes de droit souple des autorités administratives, vers l'affermissement d'une portée normative », RFDA, 2024, 467 ; Guyomar Matthias, « La hiérarchie des normes en Europe », Gaz. Pal. 12 février 2009, p. 11 ; Gény François, *Science et technique en droit privé positif*, éd. Sirey, 1921 ; Girard Charlotte, « L'accès au fondement du droit : de la technicisation des méthodes jurisprudentielles à la

le juge. L'autorité publique doit maintenir la responsabilité du contrôle et d'intervention en cas de défaillance des autorités administratives indépendantes. L'important pouvoir d'édiction de normes par les autorités administratives indépendantes ne doit pas être laissé sans contrôle.

Néanmoins, en soumettant certains actes de droit souple au contrôle de l'excès de pouvoir, le juge ouvre la voie à une nouvelle forme de normativité non explicitement habilitée par la loi et non ouvert originellement à une voie de recours[1071]. Ainsi, le juge participe à une étape supplémentaire dans un mouvement actuel et permanent de dilution des frontières du droit[1072].

2. La dilution de la norme dans l'ordre juridique

383. Distinction malaisée entre droit dur et droit souple. La distinction entre source réelle de droit et la nature du droit souple est source de confusion. Tout d'abord, les actes de droit souple et de droit dur disposent d'une « identité de fonction », c'est-à-dire influencer le comportement de leur destinataire[1073]. De manière cohérente et légitime, les juges refusent de fonder leurs décisions sur des actes de droit souple. Pourtant, ils reconnaissent parfois la production d'effets juridiques de certains de ces actes. Allant encore plus loin, la Commission européenne a déjà fondé ses positions sur ces actes, « leur conférant une normativité peu évidente à la lecture du droit primaire[1074] ». La diversité d'appellations de ces actes et leur potentielle force normative sont source d'insécurité juridique. Le système pyramidal est certes obsolète, mais le modèle en réseau se doit d'être cohérent pour être effectif.

384. « Dilution » de la norme. Auparavant, l'auteur de la norme permettait de conférer la portée normative de l'acte émis. Aujourd'hui, les frontières entre ces actes sont incertaines et mouvantes. En effet, il existe « une dilution de la norme » faisant « irruption d'un vocabulaire

---

démultiplication des autorités jurisdictionnelles », *in* Girard Charlotte (dir.), *Des droits fondamentaux au fondement du droit*, éd. Éditions de la Sorbonne, 2010, pp. 245-320.

[1071] Benezech Ludovic, *op. cit*.

[1072] Deumier Pascale, « Quand le droit souple rencontre le juge dur », RTD civ., 2016, 571 ; Benezech Ludovic, *op. cit.* : « Avec le droit souple, ce n'est donc plus officiellement la normativité juridique qui justifie la justiciabilité, mais c'est bien la justiciabilité, la possibilité d'exercer un recours et le cas échéant la possibilité offerte au juge de déclarer l'acte contraire à la légalité, qui entérine une forme nouvelle de normativité. ».

[1073] Conseil d'État, Le droit souple, étude de 2013, p. 136.

[1074] Guinard Dorian, « À propos du soft law en droit de l'Union européenne : analyses théorique et pratique », Rev. UE 2013, p. 609.

nouveau, maîtrisé, imprécis et trompeur qui fait que la régulation échappe d'abord au droit ou n'y entre que comme masquée, alors que sa fonction contraignante y est parfois en fait plus forte, plus prégnante, plus insidieuse, sans doute aussi plus universelle que celle de la réglementation d'antan[1075] ». À titre d'illustration, les lignes directrices peuvent avoir une « autorité intermédiaire » entre les actes de droit souple et les actes de droit dur[1076]. Par ailleurs, admettre l'implication des actes de droit souple dans un litige revient à troubler les caractères du droit souple[1077]. En pratique, il y aurait un « développement d'un droit encore plus souple, encore plus insaisissable, encore plus à l'abri du juge[1078] ». Le risque est alors la dilution du juridique dans l'économique puisque le droit souple se situe entre le droit dur et le non droit (sociale, morale, éthique)[1079]. Ainsi, les acteurs privés vont se servir de l'incertitude quant à l'ordonnancement juridique du réseau afin d'imposer de façon subreptice leurs intérêts particuliers[1080].

B) Les dangers de la co-production du droit

385. Intégration des intérêts et des acteurs dans la hiérarchie des normes. Lorsque les acteurs du numérique participent à l'élaboration des normes, leurs intérêts intègrent *de facto* la hiérarchie des normes (1). Par-delà l'intégration d'intérêts mercantiles, ce sont les acteurs eux-mêmes qui se fondent une place dans le système normatif (2).

1. L'intégration d'intérêts mercantiles dans l'élaboration des normes

386. Adhésion volontaire. La force normative des actes de droit souple est principalement une affaire de réception de ces normes par les acteurs[1081]. La coproduction du droit permet de privilégier la négociation dans le dessein de rechercher l'adhésion la plus large. Selon la

[1075] Gaudemet Guy, « La régulation économique ou la dilution des normes », RDP 2017, p. 23.
[1076] Loiseau Grégoire, *op. cit*., p. 722.
[1077] Bleusez Marion, « La réception du droit souple par le contentieux de droit privé », Dalloz, Justice et Cassation, 2023, 119.
[1078] Deumier Pascale, « Quand le droit souple rencontre le juge dur », RTD civ., 2016, 571.
[1079] *Ibid.*
[1080] Louvaris Antoine, « Le droit souple a trouvé ses juges : un foisonnement régulé », Justice et Cassation, 2023, 191.
[1081] Fricero Natalie « Algorithmes et nouvelle génération de droits humains. À propos de la Charte éthique européenne d'utilisation de l'intelligence artificielle dans les systèmes judiciaires et leur environnement », La semaine juridique, édition générale, n° 51, 2018, pp. 2288-2299, sur les instruments de droit souple : « l'inconvénient est que sa mise en œuvre repose sur la bonne volonté des adhérents » .

réception faite par les destinataires, les normes de droit souple franchissent ou non le seuil de la normativité[1082]. Il ne s'agit pas d'outils en marge du droit mais simplement d'une conception différente de la normativité juridique[1083]. La force normative de la norme dépend de ses effets sur les destinataires variables selon les acteurs[1084]. En effet, la co-production du droit est bénéfique lorsque les entreprises incarnent un intérêt qui n'est pas restreint à leurs propres intérêts[1085].

387. Adhésion intéressée. À propos des géants du numérique, il est évident qu'ils utilisent la promotion du droit souple dans leurs intérêts, sans réellement appliquer leurs obligations sous-jacentes[1086]. L'adhésion volontaire de respecter des normes pour la protection des données à caractère personnel des utilisateurs est un vœu pieux de la part de ces acteurs. De manière plus subtile, lorsque les acteurs adhèrent à ces normes de droit souple - qu'ils ont généralement eux-mêmes élaborées -, cela leur permet officieusement d'écarter un processus normatif contraignant[1087]. Pour eux, l'environnement numérique ne serait qu'un « laboratoire juridique, expérimentant des solutions pré-juridiques qui seraient ensuite consacrées, avec un effet retard,

---

1082 Pérès Cécile, « La réception du droit souple par les destinataires », *in* Association Henri Capitant des amis de la culture juridique française (dir.), *Le droit souple*, éd. Dalloz, 2009, p. 107.

1083 Chevallier Jacques, « Autorités administratives indépendantes et État de droit », Civitas Europa, vol. 37, n°2, 2016, pp. 143-154.

1084 Thibierge Catherine, *La force normative. Naissance d'un concept*, éd. LGDJ, 2009, p. 822 : « La force de la norme qui est perçue, ressentie ou encore vécu et conférée par ses destinataires. ».

1085 Frison-Roche Marie-Anne, « L'hypothèse de l'interrégulation », *in* Frison-Roche Marie-Anne (dir.), *Les risques de la régulation*, éd. Dalloz, 2005, p. 79 : « Cependant, comme la régulation suppose que l'on cherche un intérêt qui n'est pas restreint à l'intérêt de chaque entreprise, cela implique par définition que l'entreprise-régulateur incarne un intérêt dépassant le sien propre, selon l'idée qu'on ne peut réguler un intérêt plus grand que le sien. ».

1086 Osman Filali, « Avis, directives, codes de bonne conduite, recommandations, déontologie, éthique, etc. : réflexion sur la dégradation des sources privées du droit », RTD civ., 1995, 509 : « Ces nouveaux instruments de régulation sociale, outre le fait qu'ils posent le problème étroitement lié à ce que d'aucuns qualifient de "rôle des normes non juridiques dans le droit", montrent que les opérateurs privés, confrontés à l'impossibilité dans laquelle se trouvent les États à réglementer complètement et unilatéralement leur économie, font acte de collaboration en rédigeant des actes, constitutifs de véritables réglementations professionnelles, mais dont une partir ou la totalité est dotée d'une juridicité affaiblie, voire inexistante. Ils escomptent ainsi une moralisation de la branche par l'énoncé de "principes d'éthique professionnelle". ».

1087 Corgas-Bernard Cristina, « Les mutations de la norme en droit interne. Les règles de bonnes pratiques », *in* Martial-Braz Nathalie, Riffard Jean-Francois, Béhar-Touchais Martine (dir.), *Les mutations de la norme : le renouvellement des sources du droit*, éd. Economica, 2011, p. 79 : « La critique atteint son paroxysme lorsque cette volonté d'uniformisation dissimule des objectifs économiques, des réductions de coûts qu'elle a vocation à servir. Le double discours qui est alors tenu ne peut qu'affecter l'accessibilité de la norme de bonne pratique. Les normes de bonnes pratiques laissent enfin perplexes lorsqu'elles tendent officieusement à écarter tout processus normatif contraignant. L'hostilité de certains milieux professionnels à l'égard de l'interventionnisme législatif n'est plus à démontrer. ».

par les sources officielles du système[1088] ». Il ne faut pas écarter le fait que leur objectif est uniquement lucratif dans le dessein de développer les technologies leur permettant de faire évoluer leurs bénéfices[1089].

388. Intérêts mercantiles et techniques. À ce sujet, le Conseil de l'Europe s'inquiète de la « concentration de données, d'informations, du pouvoir et des capacités d'influence » des géants du numérique « dont les modèles d'activité privilégient les profits des actionnaires[1090] ». Les principes éthiques et l'autorégulation ne peuvent être suffisants et ne doivent aucunement intégrer le système de normes de manière prégnante[1091] : les acteurs du numérique vont pouvoir omettre volontairement les points essentiels à leur développement dans leurs normes de droit souple. La technicité de leurs pratiques leur permet d'édicter les règles dans un environnement dont ils ont le contrôle et dont ils sont les principaux acteurs[1092]. Au regard de l'inintelligibilité de leurs pratiques, le législateur - national ou européen - rencontre des difficultés à identifier les points essentiels de la législation et les omissions involontaires du législateur sont à nouveau dans l'intérêt des acteurs du numérique.

2. L'intégration des acteurs dans le système de normes

389. Pouvoir préjudiciable de création normative. La conséquence de la privatisation des normes est incontestablement l'appropriation d'un pouvoir de création normative illégitime de ces acteurs. Le danger du pouvoir de création normative par ces acteurs est leur intégration subreptice dans le réseau de normes[1093]. Pour eux, le droit souple et l'autorégulation servent

---

1088 Van de Kerchove Michel et Ost François, *De la pyramide au réseau ? Pour une théorie dialectique du droit*, Bruxelles, éd. Publications des Facultés universitaires Saint-Louis, 2002, p. 121.

1089 Benabou Valérie-Laure, « Un droit vivant. Manifeste pour des juristes incarnés et sensibles à l'heure de l'intelligence artificielle, », *Mélanges en l'honneur de Michel Vivant*, éd. Dalloz, 2020, p. 724.

1090 Assemblée parlementaire du Conseil de l'Europe, « La nécessité d'une gouvernance démocratique de l'intelligence artificielle », Résolution 2341(2020), 22 octobre 2020.

1091 Peyrou-Bartoll Sylvie, « Quelques réflexions sur les réponses institutionnelles européennes en matière d'intelligence artificielle (IA) et de robots », *in* Peyrou-Bartoll Sylvie (dir.), *Nouvelles technologies et droit européen : quel droit face à la disruption numérique ?*, éd. Mare et Martin, 2022 p. 49.

1092 Martial-Braz Nathalie, « La transdisciplinarité du droit numérique », *Mélanges en l'honneur de Michel Vivant. Penser le droit de la pensée*, p. 856.

1093 Mekki Mustapha, « Propos introductifs sur le droit souple », *Le droit souple*, *op. cit.*, p. 21 : « La dispersion et la dilution du processus normatif par l'importance croissante du droit souple facilitent l'intervention des groupes de pression et contribuent à la mise en place d'un néocorporatisme sauvage. Les groupes de pression peuvent intervenir à différents stades de la chaîne normative en toute clandestinité et de manière très discrète. ».

« d'essai » afin d'identifier les potentielles entraves à leur développement. Une fois les entraves identifiées, ils vont pouvoir cibler leur *lobbying* sur ces points précis. Allant encore plus loin dans la réflexion, le temps d'élaboration des normes leur permet - pendant les années de négociations entre les États membres - de faire perdurer leurs pratiques et d'élaborer des pratiques alternatives contournant d'ores et déjà les futures normes. Ainsi, une fois les règlements entrés en vigueur, ils ont déjà élaboré les futures technologies leur permettant de pérenniser l'exploitation des données des utilisateurs. *In fine,* la transformation du droit souple en droit dur est une opportunité espiègle pour appréhender les futures normes qu'ils ont eux-mêmes élaborées dans un premier temps.

390. Absence de légitimité des protagonistes. En réalité, les géants du numérique ne sont pas légitimes pour élaborer les normes dont ils sont les protagonistes. La technicité et la célérité des pratiques des acteurs du numérique ne doivent pas réduire l'intervention du législateur et le recul du législateur entraîne le « culte du compromis », favorable aux acteurs du numérique[1094]. Le droit souple doit redevenir complémentaire au cadre normatif. Par ailleurs, l'État doit réaffirmer sa souveraineté et exiger une transparence effective des acteurs du numérique. Les géants du numérique restent des entreprises privées dont il convient d'exiger la transparence de leurs pratiques et l'application de leur responsabilité. L'imprécision des mots et le désordre dans le réseau de normes leur sont profitables.

[1094] Chevallier Jacques, « La gouvernance, un nouveau paradigme étatique ? », Revue française d'administration publique, 2003, p. 210 : « L'État doit éviter de substituer aux acteurs sociaux. ».

391. Conclusion de la section. La nouvelle logique de gouvernance pour le droit des données est une logique en rupture avec la logique kelsienne. En effet, la gouvernance représente une mutation de la façon de gouverner dans laquelle les pouvoirs se coordonnent afin d'atteindre des consensus dans un environnement complexe. La gouvernance est un changement de paradigme dans lequel le pouvoir de l'État recule et sur lequel repose une croyance dans l'autorégulation des groupes sociaux.

Le changement de paradigme entraîne *de facto* une modification des sources du droit. Puisque le pouvoir monopolistique de l'État recule, les autorités administratives indépendantes vont détenir un pouvoir plus puissant d'édictions de normes, de contrôle et de sanction. La multiplication des organes de régulation participe à l'enchevêtrement complexe de normes dont la portée normative est fluctuante.

Les autorités administratives indépendantes élaborent des normes de droit souple et développent l'autorégulation des groupes sociaux, plus précisément des groupes privés. D'une façon utopique, les groupes privés participent à l'élaboration des normes afin de les adapter à leur environnement technique, dont ils ont la maîtrise. Le système d'autorégulation permet par la suite au législateur d'intégrer les normes de droit souple au sein du droit dur : il s'agirait d'un cercle vertueux, dominé par une logique de gouvernance.

Néanmoins, les frontières entre le droit souple et le droit dur sont de plus en plus poreuses. Par exemple, lorsque le droit souple va servir au juge afin d'estimer le degré de responsabilité d'un acteur du numérique. Dans ce cas, le droit souple sert à l'application d'une norme de droit dur par le juge. Par ailleurs, les récents règlements altèrent davantage la frontière en intégrant directement des obligations de droit souple. Le droit souple devient donc obligatoire.

En réalité, il existe un réel danger lors de l'intégration du droit souple dans les règlements : le droit souple étant en partie élaboré par des groupes privés, cela revient à intégrer les groupes privés dans le système juridique. Dépassé par l'environnement technique, l'État régresse et les intérêts des groupes privés progressent. Les groupes privés vont pouvoir se servir du droit souple comme laboratoire de normes à évincer. Dans un premier temps, l'application de ce droit souple va permettre à ces acteurs d'identifier les normes à éviter et d'appliquer un *lobbying* parfaitement ciblé. Pire encore, lorsque le législateur européen décide d'intégrer toutefois

certaines normes dans les règlements, le temps de discussions entre les États membres leur permet d'élaborer d'ores et déjà des techniques alternatives à celles qui vont être interdites.

392. Conclusion du chapitre. La logique pyramidale dominée par le monopole d'édiction des normes par l'État est une vision archaïque. Le droit des données est un droit évoluant dans un environnement complexe et contrôlé par de puissants acteurs privés. Afin de s'adapter à cet espace sans frontière, l'Union européenne détient une hégémonie remarquable sur l'élaboration des normes en matière de données. La réponse européenne était louable et nécessaire au regard de la nécessité d'harmonisation du droit applicable.

De fait, le législateur a peu à peu délégué son pouvoir normatif à des autorités de régulation. La logique kelsienne est remplacée par une logique de gouvernance afin de s'adapter à ce nouvel environnement. La gouvernance est un changement de paradigme dominé par la croyance dans l'autorégulation des groupes sociaux et le recul de l'État. Les groupes sociaux, c'est-à-dire les entreprises privées, sont les protagonistes de la technicité de leur propre environnement et sont donc les plus idoines à élaborer des normes. Depuis quelques années, la construction d'un cadre normatif pour les données est incontestablement marquée par une privatisation des normes.

Néanmoins, la privatisation des normes est un danger pour la cohérence du système juridique. Grâce à la croyance dans l'autorégulation, les acteurs privés s'imbriquent dans chaque étape de l'élaboration des normes. Ils conçoivent leurs propres règles en ayant la parfaite maîtrise de leur environnement. Cette maîtrise leur permet de se servir du droit souple comme un laboratoire de normes à évincer. L'application des normes de droit souple leur permet tout d'abord de faire l'autopromotion de l'adhésion à ces normes. Ensuite, l'adhésion et l'élaboration des normes de droit souple leur permettent de temporiser l'élaboration d'une norme de droit dur par le législateur. Ils font partie intégrante du système, censé être cohérent pour être effectif. Or, leur intérêt est de renforcer la multiplicité afin que les normes ne s'articulent pas correctement.

Pire encore, l'intégration des groupes privés dans l'élaboration des normes au profit du recul de l'État leur permet d'exercer leur *lobbying* d'une manière extrêmement précise. Avec l'application du droit souple dans un domaine identifié, ils vont pouvoir cibler les normes pouvant entacher leur développement économique. Par ailleurs, dans l'hypothèse où les groupes de pression n'arrivent pas à leur fin, ils ont déjà pu anticiper le contournement des règles avec le développement de technologies émergentes. Ainsi, l'intégration subversive des groupes privés dans le réseau de normes pose question.

Chapitre 2 : Le modèle du réseau de normes pour les données : un outil de subversion

393. Articulation souple. Le développement des usages pour les données a bouleversé le système pyramidal. Le législateur partage son pouvoir avec les autorités administratives indépendantes et ces dernières se sont multipliées afin de réguler chaque secteur. La multiplicité des autorités administratives indépendantes entraîne une multiplicité des outils de régulation. Par-delà l'émission de droit souple, une véritable logique de *compliance* s'est installée pour le droit des données. La logique de *compliance* mobilise l'ensemble des outils normatifs. En pratique, la multiplicité et la diversité de ces autorités nécessitent une articulation relativement souple et adaptable des mécanismes de régulation pour atteindre un système cohérent (**Section 1**).

394. Articulation superficielle. Néanmoins, avec le développement de la régulation et de la *compliance*, les acteurs du numérique internalisent de plus en plus les normes. L'internalisation des normes par des entreprises privées leur permet de contrôler leur environnement et le cadre normatif. La maîtrise du cadre normatif est une opportunité pour ces acteurs de contourner les règles afin de faire perdurer leurs pratiques. L'étude de ces mécanismes au regard de la maîtrise de ces acteurs permet d'identifier la superficialité des mécanismes de protection des données à caractère personnel (**Section 2**).

Section 1 : L'articulation flexible des mécanismes de régulation

395. Articulation souple. Le numérique a pratiquement transformé l'ensemble des secteurs d'activité. La transformation de ces secteurs a entraîné des modifications dans la logique de régulation traditionnelle. La logique de régulation sectorielle n'est plus adéquate au regard des flux de données : les données transcendent tous les secteurs et nécessitent la coopération des divers niveaux de régulation. Par ailleurs, les technologies évoluent rapidement dans un environnement disruptif. Ainsi, les diverses instances de régulation doivent s'articuler de façon souple afin de correspondre aux besoins du numérique (I).

La régulation des divers secteurs par les autorités administratives indépendantes permet une flexibilité dans l'application de la normativité. La logique appliquée par les autorités de régulation est prioritairement incitative afin de ne pas brider l'innovation. Ainsi, les autorités de régulation utilisent un éventail gradué de normativité afin de toujours privilégier dans un premier temps l'incitation et l'accompagnement. Pour ce faire, il existe divers instruments normatifs dont l'articulation s'avère subtile (II).

I. L'articulation souple des diverses instances de régulation

396. Diversité et multiplicité. Afin de s'adapter aux nécessités de chaque secteur, les autorités administratives indépendantes se sont développées ces deux dernières décennies. Particulièrement, l'intégration du numérique dans les différents secteurs entraîne des modifications récurrentes et complexes au sein des autorités de régulation. Le constat est celui d'une multiplicité dynamique des autorités administratives indépendantes (A). La diversité considérable de ces autorités de régulation exige de repenser leur articulation. L'instauration d'un « système de régulation en réseau » pour les autorités administratives indépendantes paraît indispensable afin de maintenir une certaine cohérence dans la régulation (B).

A) La multiplicité dynamique des autorités administratives indépendantes

397. Annonce de plan. Le mouvement de multiplication des autorités administrative indépendante s'est accentué ces dernières années (1). Les autorités administratives indépendantes sont de plus en plus nombreuses et diverses dans leur domaine d'intervention. Afin de leur garantir les moyens d'effectuer leurs missions, les pouvoirs des autorités de régulation ont évolué de façon considérable (2).

1. La diversité excessive des autorités administratives indépendantes

398. Commission nationale de l'informatique et des libertés (CNIL). Au sujet des données, la Commission nationale de l'informatique et des libertés est l'autorité de référence pour le contrôle et la régulation pour les données à caractère personnel. Première autorité indépendante française, elle est devenue une réelle autorité de supervision au sens du Règlement (UE)

2016/679 du Parlement européen et du Conseil du 27 avril 2016[1095]. À l'échelle européenne, le règlement du 18 décembre 2000 a institué le Contrôleur européen des données à caractère personnel (CEPD)[1096]. La mission du CEPD étant de veiller à l'application du RGPD dans l'ensemble des pays membres de l'Union européenne.

399. Commission d'accès aux documents administratifs (CADA). Pour les données publiques, la Commission d'accès aux documents administratifs est l'autorité de référence pour leur ouverture. La Commission a été créée par la loi n° 78-753 du 17 juillet 1978, visant à améliorer les relations entre l'administration et le public[1097]. Le rôle de cette autorité est de veiller à la liberté d'accès aux documents administratifs ainsi qu'à la réutilisation des informations publiques : elle peut être saisie par des personnes physiques ou morales lors d'un refus en matière d'accès ou de réutilisation d'informations publics. Il s'agit également de l'autorité de référence pour éclairer les administrations sur la mise en œuvre du droit d'accès ou de réutilisation.

400. Autorité de régulation de la communication audiovisuelle et numérique (ARCOM). L'ARCOM est issue de la fusion entre le Conseil supérieur de l'audiovisuel (CSA), créé en 1989, et la Haute autorité pour la diffusion des œuvres et la protection des droits sur Internet (HADOPI), créé en 2009. Les évolutions de l'environnement numérique et des technologies ont nécessité de fusionner les autorités afin de déterminer un nouveau régulateur aux compétences renforcées et élargies. La Loi n°2021-1109 du 24 août 2021 a définitivement acté le rôle dévolu à l'autorité de régulation : elle devient l'autorité de régulation de l'audiovisuelle mais aussi de la communication en général. L'autorité de régulation est garante des libertés de communication et d'expression dans les espaces numériques et dans le secteur de l'audiovisuel.

[1095] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).
[1096] Règlement (CE) n° 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données.
[1097] Loi n° 78-753 du 17 juillet 1978 portant diverses mesures d'amélioration des relations entre l'administration et le public et diverses dispositions d'ordre administratif, social et fiscal.

401. Divers organes de régulation pour l'intelligence artificielle. Récemment, le Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle met en place une « nouvelle architecture de gouvernance » [1098]. Plusieurs organes de régulation sont mis en place tels qu'un Bureau de l'intelligence artificielle au sein de la Commission, un groupe scientifique d'experts indépendants, un Comité de l'intelligence artificielle et un forum consultatif destiné aux parties prenantes[1099]. Allant encore plus loin que les « simples » autorités administratives indépendantes, le règlement sur l'intelligence artificielle instaure un véritable éventail d'instances ou « d'organes » de régulation.

402. Multiplication des autorités administratives indépendantes. Néanmoins, plusieurs rapports parlementaires insistent sur la prolifération excessive des autorités administratives indépendantes ces dernières années, relevant une certaine incohérence juridique[1100]. Pour chaque secteur spécifique, une autorité administrative indépendante est mise en place afin de

[1098] Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle et modifiant les règlements (CE) n° 300/2008, (UE) n° 167/2013, (UE) n° 168/2013, (UE) 2018/858, (UE) 2018/1139 et (UE) 2019/2144 et les directives 2014/90/UE, (UE) 2016/797 et (UE) 2020/1828 (règlement sur l'intelligence artificielle).

[1099] Commission européenne, « Législation sur l'intelligence artificielle (IA) : le Conseil donne son feu vert définitif aux premières règles mondiales en matière d'intelligence artificielle », Communiqué de presse, 21 mai 2024.

[1100] Gélard Patrice, « Les autorités administratives indépendantes : évaluation d'un objet juridique non identifié », Rapport n° 404 (2005-2006), déposé le 15 juin 2006 ; Mézard Jacques, « Un État dans l'État : canaliser la prolifération des autorités administratives indépendantes pour mieux les contrôler », Rapport n° 126, déposé le 28 octobre 2015 : « La liste des autorités administratives indépendantes s'allonge chaque année à un rythme incontrôlé, dans une indifférence générale. Pourtant, si le choix d'une telle structure peut se justifier après une solide réflexion, il n'est pas neutre pour l'organisation des pouvoirs, la capacité du contrôle du Parlement et in fine l'exercice de la responsabilité politique des décisions, parfois importantes, qui seront prises. L'extrême hétérogénéité de cette catégorie juridique met en lumière la disparité des garanties d'indépendance dont bénéficient leurs membres : les ressources financières ne sont pas toujours assurées pour l'accomplissement de leurs missions, le soutien logistique relève d'autorités extérieures, l'influence d'institutions, certes respectables mais tout autant extérieures, s'exerce. » ; Gélard Patrice, « Autorités administratives indépendantes - 2006-2014, un bilan », Rapport d'information n° 616, déposé le 11 juin 2014 : « Malgré les préconisations de l'Office parlementaire qui invitait à une réduction du nombre de ces autorités, leur rythme de création est resté soutenu. Depuis le dépôt du rapport en juin 2006, le législateur a créé onze nouvelles autorités indépendantes : l'Autorité de contrôle prudentiel et de résolution (ACPR) ; l'Autorité de régulation des activités ferroviaires (ARAF) ; l'Autorité de régulation des jeux en ligne (ARJEL) ; l'Autorité de sûreté nucléaire (ASN) ; le Comité d'indemnisation des victimes des essais nucléaires (CIVEN) ; la Commission nationale consultative des droits de l'homme (CNCDH) ; le Contrôleur général des lieux de privation de liberté (CGLPL) ; le Défenseur des droits ; la Haute Autorité pour la diffusion des oeuvres et la protection des droits sur Internet (HADOPI) ; le Médiateur national de l'énergie ; la Haute Autorité pour la transparence de la vie publique (HATVP). ».

réguler le secteur aspirant à protéger les libertés fondamentales ou à garantir le jeu de la concurrence[1101]. Néanmoins, les flux de données convergent dans tous les domaines, brouillant les compétences et domaines de chacune[1102] : les autorités administratives indépendantes rayonnent alors par « leur développement désordonné[1103] ». Leur prolifération entraîne un certain pluralisme normatif, confirmant l'obsolescence du principe pyramidal fondé sur la construction verticale de l'État de droit[1104]. Les autorités administratives doivent s'articuler entre elles en coopérant dans plusieurs domaines afin de mener une régulation cohérente pour les acteurs et surtout, pour la protection des individus.

Par ailleurs, les autorités administratives indépendantes sont de plus en plus nombreuses et de plus en plus diverses dans leurs domaines d'interventions, leurs organisations et surtout leurs pouvoirs[1105]. Le renforcement des pouvoirs des autorités de régulation était indispensable afin de mener convenablement leurs missions.

2. La diversité évolutive des pouvoirs des autorités de régulation

403. Pouvoirs des autorités administratives indépendantes. Afin d'exercer leur fonction de régulation, les autorités administratives indépendantes sont dotées de certains pouvoirs. Les pouvoirs dévolus à ces autorités de régulation vont de l'édiction de normes à un pouvoir d'investigation et de sanction. Les pouvoirs délégués aux autorités de régulation seraient contraires au principe de séparation des pouvoirs, principe central de l'édifice du droit[1106]. En réalité, les pouvoirs des autorités administratives indépendantes sont indispensables afin d'assurer une régulation efficiente du numérique[1107] et les pratiques des géants du numérique nécessitent une régulation ciblée afin de s'adapter à leurs pratiques évolutives. Ainsi, les pouvoirs de ces autorités sont amplement justifiés au regard de la puissance de ces acteurs.

1101 Chevallier Jacques, « Le statut des autorités administratives indépendantes : harmonisation ou diversification ? », RFDA, 2010, 896 ; Idot Laurence, « Une nouvelle étape dans la réalisation du marché unique des données », Europe, n° 8-9, août-septembre 2023.

1102 Benabou Valérie-Laure, « L'extension du domaine de la donnée », Legicom, n° 59, 2017, pp. 3-17.

1103 Autin Jean-Louis, « Le devenir des autorités administratives indépendantes », RFDA, 2010, 875.

1104 Chevallier Jacques, « Autorités administratives indépendantes et État de droit », Civitas Europa, n° 37, 2016, p. 149.

1105 Chevallier Jacques, « Les autorités administratives indépendantes : un produit d'importation ? », *in* Fabien Bottini (dir.), *Néolibéralisme et américanisation du droit,* éd. Mare et Martin, 2019, pp. 141-154.

1106 Chevallier Jacques, « Autorités administratives indépendantes et État de droit », op. cit, p. 148.

1107 Piwnica Emmanuel, « La dévolution d'un pouvoir de sanction aux autorités administratives indépendantes », RFDA, 2010, 915.

404. Pouvoirs de la CNIL. Tout d'abord, la Commission nationale de l'informatique et des libertés joue un rôle crucial pour le respect des normes sur la protection des données à caractère personnel[1108]. Afin de mener à bien sa mission, l'autorité est dotée d'un pouvoir d'édiction de normes. En effet, l'article 11 de la Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés dispose que l'autorité « établit et publie des règlements types en vue d'assurer la sécurité des systèmes de traitement de données à caractère personnel[1109] ». La Commission nationale de l'informatique et des libertés précise d'ailleurs que les règlements types « sont des cadres de référence contraignants » à la différence des lignes directrices ou des règlements qui ne sont pas « prescriptifs »[1110]. La Commission nationale de l'informatique et des libertés est dotée d'un pouvoir normatif en vertu d'une habilitation textuelle[1111].

405. Pouvoirs de sanction. En outre, la Commission nationale de l'informatique et des libertés dispose d'un pouvoir de sanction indispensable. L'entrée en vigueur du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) a considérablement renforcé les pouvoirs de sanction de l'autorité[1112].

[1108] Degrave Elise, « L'autorité de contrôle », *in* De Terwangne Cécile et Rosier Karen (dir.), *Le Règlement général sur la protection des données (RGPD / GDPR). Analyse approfondie*, éd. Larcier, 2018, pp. 593-611 : « Par son indépendance, son expertise et ses prérogatives singulières, l'autorité de contrôle joue un rôle crucial pour le respect du régime juridque de la protection des données. Elle est un relais pour le législateur et le gouvernement. Elle use de moyens concrets et souples pour réguler les traitements de données mis en œuvre par le secteur public et dans le secteur privé, et offre des réponses adaptées aux questions soulevées dans ce domaine, qui sont bien souvent complexes et nécessitant une réponse rapide. ».

[1109] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés , article 11, 2° b) : « En concertation avec les organismes publics et privés représentatifs des acteurs concernés, elle établit et publie des règlements types en vue d'assurer la sécurité des systèmes de traitement de données à caractère personnel et de régir les traitements de données biométriques, génétiques et de santé. A ce titre, sauf pour les traitements mis en œuvre pour le compte de l'État agissant dans l'exercice de ses prérogatives de puissance publique, elle peut prescrire des mesures, notamment techniques et organisationnelles, supplémentaires pour le traitement des données biométriques, génétiques et de santé en application du 4 de l'article 9 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 précité et des garanties complémentaires en matière de traitement de données à caractère personnel relatives aux condamnations pénales et aux infractions conformément à l'article 10 du même règlement. ».

[1110] Commission nationale de l'informatique et des libertés, « Règlements type », site disponible, en ligne : https://www.cnil.fr.

[1111] Benezech Ludovic, « Les actes de droit souple des autorités administratives, vers l'affermissement d'une portée normative », RFDA, 2024, 467.

[1112] Tran Christophe, « La CNIL dans l'environnement européen de la protection des données personnelles : renouveau d'une autorité administrative indépendante », Droit Administratif n° 1, Janvier 2022, étude 1.

Lorsque des manquements au règlement précité ou à la loi sont portés à sa connaissance, la formation restreinte de la Commission nationale de l'informatique et des libertés peut ordonner au responsable de traitement de se mettre en conformité, de satisfaire aux demandes présentées par la personne concernée d'exercer ses droits, d'imposer une limitation temporaire ou définitive du traitement, de suspendre les flux de données ou encore de prononcer une amende administrative. Pour d'aucuns, l'autorité dispose de pouvoirs « surdimensionnés », pouvant aller du simple rappel à l'ordre à la sanction pécuniaire jusqu'à 20 millions d'euros ou 4% du chiffre d'affaires annuel mondial du responsable de traitement[1113] . Néanmoins, ces pouvoirs nous semblent justifiés au regard de la puissance et des pouvoirs des entreprises ciblées. Il ne serait pas envisageable de réguler les géants du numérique sans doter les autorités de régulation d'importants pouvoirs.

406. Évolution des pouvoirs des AAI. La Loi n° 2024-449 du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique (ci-après « SREN ») a été adoptée pour se conformer aux nouveaux règlements européens sur la régulation du numérique et protéger davantage les internautes. Pour ce faire, la loi renforce les pouvoirs de plusieurs autorités administratives indépendantes. L'Autorité de régulation de la communication audiovisuelle et numérique (ARCOM), l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse (ARCEP), l'Autorité de la concurrence ou encore la Commission nationale de l'informatique et des libertés se voient conférer de nouvelles prérogatives dans la supervision de la régulation du numérique[1114]. Afin de renforcer la protection des internautes, l'article 14, II de la loi précitée reconnaît à l'ARCOM un pouvoir de mise en demeure afin d'obtenir le retrait ou la cessation de la diffusion des contenus illicites à l'encontre des éditeurs de services de communication au public en ligne et aux fournisseurs de services d'hébergement. En cas de méconnaissance ou refus du retrait du contenu illicite, l'autorité de régulation détient un pouvoir de sanction. Par ailleurs, l'article 1er de la SREN permet également à l'ARCOM de bloquer les sites pornographiques, sans décision de justice, lorsque ces derniers n'ont pas mis en place des contrôles appropriés afin de vérifier l'âge légal[1115]. Les mesures mises en place tempèrent de manière bienvenue les pouvoirs de modération privée de ces acteurs.

[1113] Martial Braz Nathalie, Rochfeld Judith et Brogli Marine, *Droit des données personnelles : les spécificités du droit français au regard du RGPD*, éd. Dalloz, 2019, p. 275.

[1114] Musson Margot, « Loi SREN : renforcement des pouvoirs de l'ARCOM et de la CNIL au service de la protection des internautes », Dalloz IP/IT, 17 juin 2024.

[1115] Loi n° 2024-449 du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique, article 1er : « L'Autorité de régulation de la communication audiovisuelle et numérique veille à ce que les contenus

407. Nouveaux pouvoirs pour la CNIL. Par ailleurs, la loi visant à sécuriser et à réguler l'espace numérique confère également de nouveaux pouvoirs à la Commission nationale de l'informatique et des libertés[1116]. Tout d'abord, de façon raisonnable, la SREN désigne la Commission nationale de l'informatique et des libertés comme l'autorité compétente pour toutes les questions relatives aux données[1117]. Plus précisément, ladite loi confie à l'autorité de régulation des données à caractère personnel la responsabilité de veiller à la bonne application des dispositions du Règlement (UE) 2022/2065 du 19 octobre 2022 du Parlement européen et du Conseil relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (DSA), particulièrement en matière de transparence de la publicité ciblée et du profilage à destination des mineurs[1118]. Pour ce faire, la Commission nationale de l'informatique et des libertés dispose de pouvoirs d'enquête et de sanction. La sanction administrative au titre du règlement sur les services numériques peut s'élever jusqu'à 6% du chiffre d'affaires annuel mondial réalisé au cours de l'exercice précédent du fournisseur de plateforme en ligne.

De surcroît, concernant la mise en œuvre du règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données (DGA), la Commission nationale de l'informatique et des libertés est désignée comme autorité compétente afin de superviser l'altruisme des données[1119]. Concrètement, lorsque les organisations sont

pornographiques mis à la disposition du public par un éditeur de service de communication au public en ligne, sous sa responsabilité éditoriale, ou fournis par un service de plateforme de partage de vidéos, au sens de l'article 2 de la loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication, ne soient pas accessibles aux mineurs. » ; Commission nationale de l'informatique et des libertés, Délibération n° 2024-067 du 26 septembre 2024 portant avis sur un projet de référentiel de l'Autorité de régulation de la communication audiovisuelle et numérique (Arcom) relatif aux systèmes de vérification de l'âge mis en place pour l'accès à certains services permettant l'accès à des contenus pornographiques.

[1116] Loi n° 2024-449 du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique.

[1117] Martial-Braz Nathalie, « La loi SREN : un texte de plus au millefeuille numérique, so frenchy ! », CCE, n° 7, Juillet-août 2024.

[1118] *Ibid*., article 59 : « Elle [la CNIL] est l'une des autorités compétentes au sens de l'article 49 du règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 relatif à un marché unique des services numériques et modifiant la directive 2000/31/ CE (règlement sur les services numériques) et pour son application. Elle veille, à ce titre, au respect des règles mentionnées au titre IV ter de la présente loi. Elle participe au comité européen des services numériques mentionné à l'article 61 du règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 précité dans les conditions prévues à l'article 7-3 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique. ».

[1119] *Ibid*., article 57 : « Elle [la CNIL] est l'autorité compétente au sens de l'article 26 du règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données et modifiant le règlement (UE) 2018/1724 (règlement sur la gouvernance des données), pour l'application du chapitre IV du même règlement. Elle veille, à ce titre, au respect des règles mentionnées au

reconnues comme organisations altruistes, elles seront autorisées à utiliser un logo conçu par l'Union européenne, marque de confiance[1120] et elles sont soumises à une série d'obligations prévues à l'article 18 du règlement sur la gouvernance européenne des données[1121]. Désormais, l'autorité de régulation de protection des données à caractère personnel possède les compétences nécessaires au contrôle du respect des obligations de ces organisations. En cas de méconnaissance de leurs obligations, la Commission nationale de l'informatique et des libertés pourra prononcer des mises en demeure, retirer le droit d'utiliser le label conçu par l'Union européenne, prononcer la radiation du registre public national, ou encore sanctionner l'organisation à une amende administrative[1122]. Les mesures sont importantes afin de protéger les individus contre des organisations potentiellement malveillantes. Le principe de partage des données doit être surveillé afin de garantir l'altruisme des organisations.

Ainsi, les diverses autorités administratives indépendantes disposent de pouvoirs renouvelés afin de protéger davantage les utilisateurs et de sanctionner efficacement les manquements des opérateurs. Néanmoins, la diversité excessive de ces autorités peut être source de complexité[1123]. Il est nécessaire de déceler une certaine articulation entre les différentes autorités au sein de ce système de régulation en réseau.

titre IV bis de la présente loi et dispose des pouvoirs mentionnés à l'article 20-1. Ses membres et les agents de ses services habilités dans les conditions définies au second alinéa de l'article 10 peuvent constater les manquements aux exigences énoncées au chapitre IV du règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 précité. ».

[1120] Perray Romain et Favreau Julie, « Data Governance Act : le cerbère de la réutilisation des données ? », CCE, n° 3, Mars 2023.

[1121] Règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données (règlement sur la gouvernance des données), article 18, « Conditions générales d'inscription » : « Afin d'être admissible à l'inscription dans un registre national public d'organisations reconnues en matière d'altruisme en matière de données, une entité doit : (a) mener des activités d'altruisme en matière de données ; (b) être une personne morale constituée conformément au droit national pour répondre à des objectifs d'intérêt général tels que prévus par le droit national, le cas échéant ; (c) fonctionner sur une base non lucrative et être juridiquement indépendant de toute entité fonctionnant sur une base lucrative ; (d) mener ses activités d'altruisme en matière de données à travers une structure fonctionnellement distincte de ses autres activités ; (f) se conformer aux règles visées à l'article 22, paragraphe 1, au plus tard 18 mois après la date d'entrée en vigueur des actes délégués visés audit paragraphe. ».

[1122] Schwartz Julie et Schlich Rémy, « Loi SREN : de nouveaux pouvoirs pour la CNIL », Cahiers de droit de l'entreprise n° 3, Mai-Juin 2024.

[1123] Brisson Jean-François, « La diversité des régulateurs nationaux sectoriels », RFDA, 2014, 869.

B) La constitution progressive d'un système de régulation en réseau

408. Hiérarchie entre les instances de régulation. Afin de maintenir une certaine cohérence dans le réseau de normes, il est possible de déceler une hiérarchie entre les autorités de régulation. En effet, les instances de régulation interagissent dans un rapport de régulation en réseau : les autorités administratives indépendantes doivent s'interréguler au niveau national (1). Le système de réseau est également promu au niveau européen, avec l'instauration d'un mécanisme innovant de coopération (2).

1. L'inévitable mécanisme d'interrégulation au niveau national

409. Définition de l'interrégulation. La notion d'interrégulation est prégnante pour l'articulation des différentes autorités administratives indépendantes dans le domaine du numérique. Pour la Professeure Marie-Anne Frison-Roche, l'interrégulation est un moyen d'atteindre un but, c'est-à-dire de « dégager des solutions qui prennent en considération plusieurs régulations autarciques, égalitaires et divergentes, ayant chacune une légitimité à régir la situation en cause[1124] », nécessitant la mise en place de « réseaux entre des autorités demeurées autonomes[1125] ». D'une manière plus large, l'interrégulation peut être définie comme « la capacité pour une autorité de régulation de nouer des relations avec une autre autorité de régulation afin de prendre une position ou produire une décision interrégulée[1126] ». En effet, l'environnement numérique et les flux de données transcendent quasiment l'ensemble des secteurs régulés[1127] : il est évident pour le numérique que les différents secteurs régulés échappent aux frontières physiques[1128]. Afin de garantir une cohérence entre la régulation des

[1124] Frison-Roche Marie-Anne, « L'hypothèse de l'interrégulation », *in* Frison-Roche Marie-Anne (dir.), *Droit et économie de la régulation*, éd. Presses de Sciences Po, 2005, p. 70.
[1125] De Saint Pulgent Maryvonne, « Les besoins d'interrégulation engendrés par Internet », *in* Frison-Roche Marie-Anne (dir.), *Internet, Espace d'interrégulation*, éd. Dalloz, 2016, p. 3.
[1126] Delzangles Hubert, « La notion d'interrégulation », *in* Eckert Gabriel et Kovar Philippe (dir.), *L'interrégulation*, éd. L'Harmattan, 2017, p. 16.
[1127] Frison-Roche Marie-Anne, *op. cit*., p. 4 : « Dans tous les secteurs, le numérique, qui permet une mise en données du monde, manifeste sa capacité à bouleverser les règles du jeu et les positions établies et exige de repenser la régulation. […] La naissance de la nécessité de l'interrégulation procède aujourd'hui d'un souci sinon d'unification du moins de mise en cohérence des différents niveaux qui ne peuvent plus demeurer dans une juxtaposition confinant à l'ignorance. ».
[1128] Ziller Jacques, « L'interrégulation dans le contexte de l'intégration européenne et de la mondialisation », Revue française d'administration publique, 109, Institut national du service public, 2004, p. 17.

différents secteurs et surtout, de garantir une protection effective des individus, l'interrégulation des autorités administratives indépendantes était inévitable.

410. La nécessité d'interrégulation. Au sein de ce nouvel environnement, les secteurs s'entrecroisent et nécessitent une interrégulation entre différentes autorités administratives indépendantes. En effet, la prise en compte des technologies émergentes peut conduire à des chevauchements de compétence entre les différentes autorités[1129]. Ainsi, l'interrégulation se matérialise par l'organisation d'un système en réseau[1130] : grâce à ce réseau, les différentes autorités administratives indépendantes vont pouvoir coopérer et communiquer mutuellement des informations. L'interrégulation permet de pallier « le risque d'une action publique mal coordonnée, trop éclatée et excessivement complexe[1131] ». Au sujet des données et la primauté théorique des données à caractère personnel, les autorités administratives indépendantes peuvent se mettre en lien avec la Commission nationale de l'informatique et des libertés afin de coordonner leurs actions[1132].

411. Interrégulation des différentes autorités administratives indépendantes. À titre d'illustration, la Commission nationale de l'informatique et des libertés et la Commission d'accès aux documents administratifs ont publié en 2019 un guide sur l'*open data* pour la publication et la réutilisation des données publiques[1133]. Avec l'impulsion politique de l'ouverture des données, l'interrégulation entre les deux autorités est essentielle puisque les données publiques peuvent contenir des données à caractère personnel. De ce fait, les deux autorités ont coopéré afin d'établir ce guide à des fins pédagogique pour les potentiels utilisateurs. Plus récemment, en 2023, la Commission nationale de l'informatique et des libertés

---

1129 Sauvé Jean-Marc, « Les autorités administratives indépendantes », Intervention du 11 février 2010 de Jean-Marc Sauvé, audition par Christian Vanneste et René Dosière, rapporteurs de la mission mise en place par le Comité d'évaluation et de contrôle des politiques publiques (CEC) sur les autorités administratives indépendantes, 11 février 2010 : « L'interdépendance croissante entre les contenus audiovisuels et les communications électroniques, qui pose la question de la répartition des compétences entre le Conseil supérieur de l'audiovisuel (CSA) et l'autorité de régulation des postes et des communications électroniques (ARCEP) en est un exemple. ».

1130 Falque-Pierrotin Isabelle, « La CNIL face à l'économie de la donnée », D., 2015, 2432.

1131 Sauvé Jean-Marc, « Le droit de la régulation économique », Colloque organisé par l'association des Conseils d'État et des juridictions administratives suprêmes de l'Union européenne, 16 juin 2014.

1132 Favro Karine, « La CNIL, une autorité à "l'âge de la maturité" », Dalloz IP/IT, 2018, 464.

1133 Commission nationale de l'informatique et des libertés et Commission d'accès aux documents administratifs en association avec Etalab, « Guide pratique de la publication en ligne et la réutilisation des données publiques ("open data") », publié le 17 octobre 2019.

et la Commission d'accès aux documents administratifs se sont réunies exceptionnellement pour échanger au sujet du partage et de la publication des données[1134].

Au sujet des assistants vocaux et des enceintes connectés, la Haute Autorité pour la diffusion des œuvres et la protection des droits sur Internet (HADOPI) et Conseil Supérieur de l'Audiovisuel (CSA) s'étaient également associés afin de mener une étude commune à ce sujet en 2019[1135]. Finalement, au regard des enjeux intersectoriels, l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse (ARCEP), l'Autorité de la concurrence et la Commission nationale de l'informatique et des libertés se sont intégrés à la réflexion afin d'établir une étude complète[1136]. L'interrégulation est parfaitement illustrée dans cette étude où les compétences de chaque autorité administrative indépendante étaient nécessaires pour une réflexion commune.

412. Interrégulation pour l'intelligence artificielle. Au sujet de l'intelligence artificielle, une étude du Conseil d'État souligne « la très forte adhérence entre la régulation des systèmes d'intelligence artificielle et celle des données, en particulier des données à caractère

1134 Commission nationale de l'informatique et des libertés, « La CADA et la CNIL se sont réunies en un collège exceptionnel le 20 avril 2023 », 2023, disponible sur le site de la Commission nationale de l'informatique et des libertés.

1135 La Haute Autorité pour la diffusion des œuvres et la protection des droits sur Internet et Conseil Supérieur de l'Audiovisuel, Rapport « Assistants vocaux et enceintes connectés, l'impact de la voix sur l'offre et les usages culturels et médias », publié le 28 mai 2019.

1136 Rapport, *op. cit.*, p.12 : « Outre le CSA et l'Hadopi, les enjeux liés aux assistants vocaux et aux enceintes connectées intéressent également d'autres autorités de régulation, chacune dans leur champ de compétence respectif. Le fonctionnement de ces appareils repose sur une collecte importante de données personnelles, par le simple enregistrement des requêtes vocales comme par l'analyse du contenu de ces requêtes. Dès lors, les choix techniques et économiques des entreprises concernées intéressent au premier chef la Commission nationale de l'informatique et des libertés (CNIL), qui a déjà produit des analyses sur ces sujets. L'Autorité de régulation des communications électroniques et des postes (Arcep), en charge du respect de la neutralité du net, c'est-à-dire de l'égalité de traitement et d'acheminement de tous les flux d'information sur Internet est également concernée : elle relève, dans son rapport sur les terminaux, que les assistants vocaux proposent une "expérience intelligente mais orientée de l'Internet", avec le risque de voir les utilisateurs "enfermés" dans des univers de marques distribuant à la fois les terminaux, les contenus et éventuellement les services. L'Autorité de la concurrence est, quant à elle, notamment intéressée par la position concurrentielle des différents fabricants d'enceintes connectées et la pression concurrentielle qui s'exerce sur eux, par le rôle des données et des algorithmes dans la performance des terminaux, par les conditions d'accès aux terminaux pour les fournisseurs de services, par l'existence ou non d'accords d'exclusivités entre fabricant d'enceintes et fournisseur de contenus, ainsi que par les coûts de changement de terminal pour l'utilisateur. », disponible https://www.hadopi.fr.

personnel[1137] ». En janvier 2023, la Commission nationale de l'informatique et des libertés a créé un service de l'intelligence artificielle afin de renforcer son expertise dans ce domaine[1138]. Le service de l'intelligence artificielle a pour mission de contrôler l'entrée en application du règlement et de développer des relations avec les acteurs de l'écosystème. Il s'agit donc d'anticiper l'interrégulation nécessaire entre le développement de l'intelligence artificielle et les enjeux de protection des données à caractère personnel.

413. Instauration d'une hiérarchie interne entre les autorités administratives indépendantes. En allant encore plus loin, il existe désormais une hiérarchie entre les autorités administratives indépendantes elles-mêmes. En effet, la Loi n° 2024-449 du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique (SREN) désigne l'ARCOM comme « coordinateur des services numériques » en France. Ainsi, en matière de régulation de l'environnement numérique, ladite autorité devient l'autorité de coordination. La régulation de cet environnement s'effectuera donc par l'interrégulation entre l'ARCOM, la Commission nationale de l'informatique et des libertés (CNIL) au sujet de la vie privée et la Direction générale de la concurrence, de la consommation et de la répression des fraudes (DGCCRF), en ce qui concerne les dispositions spécifiques aux places de marchés. Il reste à espérer que l'articulation soit efficiente afin que les acteurs du numérique « ne se jouent de la multitude[1139] ». En effet, dans l'hypothèse où les différents pouvoirs des autorités ne s'articulent pas correctement, les acteurs du numérique pourront échapper à certaines sanctions. L'articulation des autorités de régulation est indispensable afin de mener à bien la régulation et sanctionner efficacement les sociétés qui ne respectent pas les normes instaurées. Dans le cas contraire, les géants du numérique pourront effectivement se jouer de la multitude et profiter de l'incohérence du système de régulation en réseau.

1137 Conseil d'État, Rapport « S'engager dans l'intelligence artificielle pour un meilleur service public », Actualités, 30 août 2022.

1138 Commission nationale de l'informatique et des libertés, « Création d'un service de l'intelligence artificielle à la CNIL et lancement des travaux sur les bases de données d'apprentissage », janvier 2023, disponible en ligne : « Le service de l'intelligence artificielle (SIA) créé au sein de la CNIL réunira 5 personnes. Composé de juristes et d'ingénieurs spécialisés, ce service sera rattaché à la direction des technologies et de l'innovation de la CNIL dont le directeur, Bertrand Pailhes, était précédemment coordonnateur national pour la stratégie d'intelligence artificielle au sein de la Direction interministérielle du numérique et du SI de l'État (DINSIC). » .

1139 Martial-Braz Nathalie, *op. cit*.

Pour ce faire, l'interrégulation doit également s'effectuer à l'échelle européenne. Plusieurs mécanismes sont mis en place afin de garantir une cohérence entre les différents niveaux de régulation.

2. L'innovant mécanisme de coopération au niveau européen

414. Coopération multilatérale des diverses instances. Au niveau européen, il existe également plusieurs instances européennes de régulation dans différents domaines. Le Comité européen de la protection des données (CEPD) est le successeur du groupe G29 et a été institué par le Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données[1140]. Le Comité européen pour les données à caractère personnel est un organe indépendant permettant de garantir sa légitimité[1141]. La mission principale du Comité est de superviser une application cohérente du règlement sur la protection des données à caractère personnel[1142]. Pour cela, il organise la coopération entre les différentes instances de régulation des données à caractère personnel. Le Règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données (règlement sur la gouvernance des données) a quant à lui institué un Comité européen de l'innovation dans le domaine des données. Le comité européen de l'innovation en matière de données devrait coopérer avec les organismes, réseaux ou groupes d'experts sectoriels, ou d'autres organisations intersectorielles traitant de la réutilisation des données[1143]. *In fine*, il s'agit à nouveau de faciliter la coopération entre les autorités compétentes des États membres.

1140 Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), article 68.

1141 De Terwangne Cécile et Rosier Karen, *Le règlement général sur la protection des données*, éd. Larcier, 2018, p. 616.

1142 Robert Romain, « Le Comité européen de la protection des données : le garant d'un nouvel ordre ? », *in* De Terwagne Cécile et Rosier Karen (dir.), *Le règlement sur la protection des données (RGPD/GDPR). Analyse approfondie*, éd. Larcier, 2018, pp. 613-635.

1143 Règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données (règlement sur la gouvernance des données), article 29.

415. Comité européen de l'intelligence artificielle. Enfin, le Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle a créé un Comité européen de l'intelligence artificielle (CEIA)[1144]. À l'instar des divers comités européens, le Comité conseille et assiste la Commission et les États membres afin de faciliter l'application cohérente du règlement. Il veille à ce titre à la coordination pertinente entre les différentes autorités nationales compétentes en coopération avec les autorités de surveillance du marché concernées[1145]. Il est également possible de citer le BEREC (Body of European Regulators for Electronic Communications), un organisme expert chargé d'assister la Commission européenne et les autorités réglementaires nationales. L'organisme a rendu en 2022 un rapport sur les défis et les avantages des solutions d'intelligence artificielle (IA) dans le secteur des télécommunications[1146]. Il existe donc un véritable enjeu d'articulation horizontale pour ces différentes instances européennes[1147]. Pour l'articulation verticale, les instances européennes sont « prioritaires » aux instances nationales. À titre d'illustration, le Comité européen est prioritaire sur les autorités nationales de contrôle. Afin de garantir une harmonie pour l'application du règlement sur le territoire européen, un mécanisme de coopération est prévu par le règlement.

416. Mécanisme de coopération et de cohérence pour les autorités de régulation des données à caractère personnel. Pour les traitements « transfrontaliers[1148] », le législateur européen a créé la notion de « chef de file », autorité seule compétente par principe. Autrement

---

1144 Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle et modifiant les règlements (CE) n° 300/2008, (UE) n° 167/2013, (UE) n° 168/2013, (UE) 2018/858, (UE) 2018/1139 et (UE) 2019/2144 et les directives 2014/90/UE, (UE) 2016/797 et (UE) 2020/1828 (règlement sur l'intelligence artificielle), article 65.

1145 *Ibid*., article 66.

1146 BEREC, « Draft Report on challenges and benefits of Artificial Intelligence (AI) solutions in the telecommunications sector (including use cases) », Rapport, BoR(22) 191, 12 décembre 2022.

1147 Cassar Bertrand, Plédel Chloé et Galbois-Lehalle Diane, « L'articulation du projet de règlement sur l'intelligence artificielle avec le droit du numérique européen », Dalloz IP/IT, 17 juillet 2023.

1148 Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), article 4, point 23 : "traitement transfrontalier", a) un traitement de données à caractère personnel qui a lieu dans l'Union dans le cadre des activités d'établissements dans plusieurs États membres d'un responsable du traitement ou d'un sous-traitant lorsque le responsable du traitement ou le sous-traitant est établi dans plusieurs États membres ; ou b) un traitement de données à caractère personnel qui a lieu dans l'Union dans le cadre des activités d'un établissement unique d'un responsable du traitement ou d'un sous-traitant, mais qui affecte sensiblement ou est susceptible d'affecter sensiblement des personnes concernées dans plusieurs États membres. ».

dit, lorsqu'un traitement est transfrontalier, la compétence revient à l'autorité de contrôle de l'État membre dans lequel est situé soit l'établissement « unique » du responsable du traitement ou du sous-traitant, soit lorsqu'il existe plusieurs établissements au sein de l'Union européenne, l'établissement « principal » de ce responsable[1149] : cette procédure de simplification permet à l'autorité désignée comme chef de file d'être seule compétente[1150]. Surtout, l'autorité principale pourra coopérer avec les autres autorités nationales de contrôle concernées par ce traitement[1151]. Le mécanisme de coopération a été institué par le règlement sur la protection des données, mécanisme « innovant » ayant pour dessein de permettre une application cohérente du règlement[1152]. Le mécanisme est innovant car il repose à la fois sur un mécanisme intégré et décentralisé : l'exercice conjoint des autorités est décentralisé mais intégré car la norme est identique sur tout le territoire de l'Union européenne[1153]. À titre d'illustration, la coopération va servir à soumettre le projet aux autres autorités avant avis définitif ou encore de prendre en compte le point de vue de chaque autorité[1154]. Il s'agit réellement d'un processus de discussion afin d'obtenir un consensus entre les autorités concernées. En cas de désaccord, c'est le comité européen qui rendra un avis contraignant. En pratique, ce mécanisme peut entraîner des risques de *forum shopping* pour les acteurs internationaux. Le mécanisme de coopération est intéressant, il peut toutefois devenir dangereux selon l'autorité de régulation impliquée[1155].

1149 *Ibid*., article 56.1 : « Sans préjudice de l'article 55, l'autorité de contrôle de l'établissement principal ou de l'établissement unique du responsable du traitement ou du sous-traitant est compétente pour agir en tant qu'autorité de contrôle chef de file concernant le traitement transfrontalier effectué par ce responsable du traitement ou ce sous-traitant, conformément à la procédure prévue à l'article 60. ».

1150 Gufflet Myriam, « Les efforts des autorités nationales et du Comité européen de la protection des données pour une application efficace du RGPD », l'Observateur de Bruxelles, n° 132, 2023/2, p. 23.

1151 *Ibid.*, article 60 : « L'autorité de contrôle chef de file coopère avec les autres autorités de contrôle concernées conformément au présent article en s'efforçant de parvenir à un consensus. L'autorité de contrôle chef de file et les autorités de contrôle concernées échangent toute information utile. ».

1152 Lafity Elise, « L'articulation des mécanismes de régulation en protection des données personnelles », *in* Bensamoun Alexandra, Bertrand Brunessen et Anca Ailincai Mihaela (dir.), *Le règlement général sur la protection des données : aspects institutionnels et matériels*, éd. Mare & Martin, 2020, p. 244.

1153 Louvaris Antoine, « Droits fondamentaux et innovation : quelle régulation à l'ère numérique ? », Les nouveaux cahiers du Conseil constitutionnel, n° 52, p. 7.

1154 Pouillaude Sibylle, « "Attraper les GAFAM" ou le guichet unique en droit de la protection des données personnelles : fonctionnement, bilan et perspectives », RAE, n° 2023/1, pp. 127-151, évoquant une « architecture procédurale innovante ».

1155 *Infra*., n° 601.

417. Interrégulation des régulateurs européens. À l'instar du réseau évoqué des autorités administratives indépendantes, il existe également un « réseau de régulateurs européens[1156] ». Il est possible de constater l'émergence d'un modèle européen d'interrégulation au sujet des données à caractère personnel[1157]. Le Comité européen de la protection des données coopère avec d'autres autorités dans divers domaines afin d'être cohérent dans son contrôle. En effet, le CEPD a proposé la mise en place du « Digital Clearing House », un centre d'échange d'informations sur le *Big Data* et le numérique : il s'agit de réunir les domaines de la concurrence, de la consommation et la protection des données dans l'objectif de protéger davantage les individus. Il est précisé que « tous les régulateurs de l'espace numérique, basés dans l'Union européenne ou dans le monde, sont invités à prendre part aux discussions[1158] ».

418. Interaction des données dans le cadre réglementaire. Récemment, dans un communiqué du 18 avril 2024, le Comité européen de la protection des données à caractère personnel précise que la priorité est mise sur l'interaction des données avec le nouveau cadre réglementaire numérique. Les nouveaux règlements tels que le Règlement (UE) 2022/1925 du Parlement européen et du Conseil du 14 septembre 2022 relatif aux marchés contestables et équitables dans le secteur numérique (DMA) et le Règlement (UE) 2022/2065 du 19 octobre 2022 du Parlement européen et du Conseil relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (DSA) ont un impact sur la protection des données, ainsi le Comité s'engage à renforcer la coopération avec les autres autorités de régulation, « en vue d'intégrer le droit à la protection des données dans l'architecture réglementaire globale[1159]». Il précise également qu'il accordera une attention particulière aux nouveaux défis posés par l'intelligence artificielle. L'un des objectifs de sa stratégie jusqu'à 2027 est de contribuer au dialogue mondial sur la protection des données. Par-delà l'interrégulation européenne, l'ouverture est désormais mondiale afin de s'adapter à l'échelle réelle du défi numérique.

1156 Idoux Pascale, « Régulateurs nationaux et régulateurs européens », Revue du droit public, n°2, 2014, p. 290.

1157 Tambou Olivia, « L'émergence d'un modèle européen d'interrégulation en matière de protection des données personnelles », *Liber Amicorum en l'honneur du professeur Joël Monéger,* Lexis Nexis, 2017.

1158 Contrôleur européen de la protection des données, disponible sur : https://www.edps.europa.eu/data-protection/our-work/subjects/big-data-digital-clearinghouse_en.

1159 Comité européen des données à caractère personnel, « EDPB Strategy 2024-2027 », 24 avril 2024, dont il ressort 4 piliers : Renforcer l'harmonisation et promouvoir la conformité ; Renforcer une culture commune de l'application et une coopération efficace ; Sauvegarder la protection des données dans le paysage numérique et interréglementaire en développement ; Contribuer au dialogue mondial sur la protection des données. ».

419. Articulation théorique entre les autorités. Ainsi, les autorités européennes s'interrégulent à l'échelle de l'Union européenne mais également entre les autorités européennes et les autorités de contrôle nationales afin de prendre en compte l'ensemble des domaines impactés par le numérique et les données. L'articulation s'effectue par niveau entre les autorités et d'une manière verticale entre les autorités européennes et nationales[1160]. L'articulation entre les autorités de contrôle est indispensable : seule une articulation appropriée pourra contrer le pouvoir et l'influence des acteurs du numérique. *In fine*, l'articulation entre ces autorités permet une application cohérente du cadre normatif. Par ailleurs, l'articulation entre les divers instruments normatifs est également primordiale.

II. L'articulation subtile des divers instruments normatifs

420. Régulation privatisée. L'émergence et la diversité des autorités de régulation a pour dessein de réguler de façon plus souple les acteurs du numérique. Avec l'opacité et la technicité de leurs pratiques, le droit souple se développe afin de s'adapter à la célérité des technologies. Le droit souple parait idoine dans la mesure où il permet de ne pas ralentir le développement des technologies émergentes. Afin d'internaliser cette flexibilité dans les entreprises, un véritable système de *compliance* s'est mis en place ces dernières années (A). Les autorités de régulation conservent une place déterminante en élaborant les normes de droit souple utilisées en partie dans la *compliance*. En pratique, plus la c*ompliance* et la régulation se renforcent, plus le pouvoir normatif des autorités de régulation s'intensifie (B).

A) La mise en place innovante d'un système de *compliance*

421. Mécanisme de *compliance*. Le système de *compliance* utilise toute la gamme de normativité des outils de droit souple au droit dur. Tout d'abord, les acteurs vont apprécier les risques de leurs activités afin d'incorporer les normes au sein de leur structure (1). Il s'agit de responsabiliser les acteurs par l'incitation plutôt que par la contrainte. Toutefois, en cas de méconnaissance des règles ou des procédures à mettre en place, le droit dur (re)devient l'outil adapté afin de sanctionner les acteurs (2).

[1160] Bertrand Brunessen, « La Cour de justice, régulateur de la gouvernance institutionnelle du RGPD », Dalloz actualité, 30 juin 2021.

1. L'internalisation utopique des normes par les acteurs

422. Notion de *compliance*. La logique de *compliance* appliquée aux secteurs financiers et bancaires est transposée au droit du numérique[1161]. La *compliance* prolonge la régulation qui s'était elle-même substituée en partie à la réglementation[1162] : cette logique confirme le recul de l'État en renforçant le pouvoir des acteurs du numérique. L'application de la norme est moins dans une logique verticale et devient plus intégrée directement par les opérateurs[1163]. En effet, les normes de *compliance* ont pour objet de modifier ou d'orienter les comportements des acteurs économiques[1164]. Il ne s'agit plus de contraindre les opérateurs mais de les inciter à respecter un ensemble de normes destinées à atteindre un but[1165]. Pour parvenir à ces « buts monumentaux », la *compliance* va se servir de toute la gamme de normativité. Partant du droit souple, ce mouvement use également des normes de droit dur afin de garantir une certaine effectivité. Finalement, l'ensemble des normes va corréler à une unité vers le but recherché[1166].

423. L'internalisation des normes en matière de données à caractère personnel. En matière de données à caractère personnel, le but recherché est la protection des individus et la protection de la vie privée. Partant de ce but, les acteurs économiques vont devoir internaliser les normes afin de respecter cet objectif. En revanche, lors d'un contrôle, ils devront attester du respect des normes et de la protection des données, tout au long du processus. À titre d'illustration, la logique d'*accountability* introduite dans le règlement sur la protection des données recouvre une logique de *compliance*[1167]. En effet, le responsable du traitement est responsable et surtout, il doit être en mesure de démontrer le respect des obligations lui

---

[1161] Iliopoulou-Penot Anastasia, « La Constitution numérique européenne », RFDA, 2023, 945 .

[1162] Conseil d'État et Cour de cassation, De la régulation à la compliance : quel rôle pour le juge ?, *Regards croisés du Conseil d'État et de la Cour de cassation*, éd. La documentation française, 2024, p. 14.

[1163] Bertrand Brunessen et Sirinelli Jean, « L'approche comportementale dans la régulation du numérique », *Entre art et technique : les dynamiques du droit: mélanges en l'honneur de Pierre Sirinelli*, éd. Dalloz, 2022, p. 576.

[1164] Morel-Maroger Juliette, « La réception des normes de la compliance par les juges de l'Union européenne », *in* Frison-Roche Marie-Anne et Ancel François (dir.), *La juridictionnalisation de la compliance*, éd. Dalloz, 2023, p. 443.

[1165] Frison-Roche Marie-Anne, *Les buts monumentaux de la compliance*, éd. Dalloz, 2022.

[1166] Frison-Roche Marie- Anne, « Approche juridique des outils de la compliance. Construire juridiquement l'unité des outils de la compliance à partir de la définition du Droit de la compliance par ses "buts monumentaux" », *in* Frison-Roche Marie-Anne (dir.), *Les outils de la compliance*, éd. Dalloz, 2021, p. 27.

[1167] Falque-Pierrotin Isabelle, « L'Europe des données ou l'individu au cœur d'un système de compliance », *in* Frison-Roche Marie-Anne (dir.), *Régulation, Supervision, Compliance*, éd. Dalloz, 2017, pp. 29-33.

incombant[1168]. Dans un premier temps, il revient au responsable de traitement de se conformer aux obligations du règlement, c'est-à-dire respecter les principes relatifs aux traitements des données à caractère personnel. Pour ce faire, une certaine liberté est accordée aux responsables de traitement. Ils peuvent décider d'élaborer eux-mêmes des normes en interne afin de maintenir une cohérence dans l'ensemble de l'entreprise, ou ils peuvent appliquer les normes de droit souple édictées par les autorités de régulation[1169]. En tout état de cause, l'essentiel est le respect des normes et la protection des individus[1170] : en cas de contrôle le responsable de traitement doit démontrer le respect des principes tout au long des traitements[1171]. Les acteurs économiques sont donc « responsabilisés » dans une logique de confiance. Finalement, qu'importe la nature de la norme appliquée, l'essentiel étant le respect des principes[1172]. Les récents règlements européens ont majoritairement intégré des logiques de *compliance* parmi les obligations réglementaires[1173].

424. Risques de la *compliance*. Il revient alors aux opérateurs économiques d'analyser les risques de leurs pratiques afin de mettre en place les mesures adéquates : « faussement simple, l'approche par les risques s'appuie sur une articulation complexe entre différents instruments juridiques[1174] ». En réalité, la complexité est souvent bénéfique aux opérateurs économiques. Logiquement, il est préférable pour ces opérateurs de respecter les principes de *compliance*

1168 Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), article 5, paragraphe 2 : « Le responsable du traitement est responsable du respect du paragraphe 1 et est en mesure de démontrer que celui-ci est respecté (responsabilité). ».

1169 Maxwell Winston et Taïeb Sarah, « L'accountability, symbole d'une influence américaine sur le règlement européen des données personnelles ? », Dalloz IP/IT, 2016, 123.

1170 Falque-Pierrotin Isabelle, « L'Europe des données ou l'individu au coeur d'un système de compliance », *in* Frison-Roche Marie-Anne (dir.), *Régulation, Supervision, Compliance*, éd. Dalloz, 2017, pp. 29-33.

1171 Gola Romain, « Le règlement européen sur les données personnelles, une opportunité pour les entreprises au-delà de la contrainte de conformité », Légicom, 2017, 29 .

1172 Lamon Bernard, « Le principe d'"accountability" et les instruments de mise en conformité », *in* Bensamoun Alexandra, Bertrand Brunessen et Anca AilincaiI Mihaela (dir.), *Le règlement général sur la protection des données : aspects institutionnels et matériels*, éd. Mare & Martin, 2020, p. 221.

1173 Lequette Suzanne, *Droit du numérique*, éd. LGDJ, 2024, p. 47 : « En d'autres termes, à la logique traditionnelle logique verticale et hiérarchique du processus normatif se voit substituer une logique horizontale fondée sur la coopération entre les pouvoirs publics et les opérateurs. Ayant principalement émergé à l'origine dans le secteur de la finance, ce nouveau type de régulation trouve désormais un terrain d'application privilégié avec le numérique dès lors qu'il permet au pouvoir normatif de faire peser le poids de la prévention des risques que peuvent engendrer cette technologie sur les opérateurs qui la mettent en œuvre. ».

1174 Latil Arnaud, *Le droit du numérique. Une approche par les risques*, éd. Dalloz, 2023, p. 3.

plutôt que d'être soumises à un carcan réglementaire[1175]. En pratique, toute la logique de *compliance* repose sur l'opacité des techniques de ces opérateurs.

Dans l'environnement numérique, la *compliance* a été intégrée en réponse à l'incapacité du législateur à déceler les normes à élaborer. La *compliance* devient l'unique solution pour moraliser les acteurs grâce à leur propre implication[1176]. En effet, au regard de l'opacité volontaire, le législateur n'arrive pas à encadrer ces pratiques. Il revient alors aux opérateurs de trouver les remèdes à leurs propres maux, aux risques systémiques[1177] : de ce fait, l'efficacité de la régulation dépend de la bonne foi des entreprises concernées[1178]. La frontière entre le bien et le mal est par conséquent entre leurs mains, pourtant « il est probable que la poursuite du bien commun ne soit pas la préoccupation première des personnes qui conçoivent des systèmes d'intelligence artificielle ou des entreprises qui les commercialisent[1179] ».

Ainsi, la poursuite des « buts fondamentaux » - raison d'être de la *compliance* -, ne peut être laissée entre les mains d'opérateurs économiques. En matière de protection des données à caractère personnel, le but ultime de protection des individus n'est pas l'objectif de ces acteurs. Les « buts fondamentaux » de ces opérateurs se retrouvent davantage dans un objectif économique. En admettant l'absence de similarité entre les buts fondamentaux de la *compliance* entre le législateur et les opérateurs économiques, la logique de *compliance* devient simplement

---

1175 Marti Gaëlle, « Les instruments normatifs de la politique du numérique », *in* Bertrand Brunessen (dir.), *La politique européenne du numérique*, éd. Bruylant, 2023, p. 244.

1176 Favro Karine, « La démarche de compliance ou la mise en œuvre d'une approche inversée », Legicom, n° 59, 2017.

1177 Tinière Romain, « L'Union européenne et la régulation des plateformes en ligne - à la recherche de la voie du milieu », *in* Bertrand Brunessen (dir.), *La politique européenne du numérique,* éd. Bruylant, 2023, p. 704.

1178 Auby Jean-Bernard, « Le dialogue de la norme étatique et de la compliance », *in* Frison-Roche Marie Anne (dir.), *Régulation, supervision, compliance*, éd. Dalloz, 2017, p. 105 : « Elle [la compliance] présente l'inconvénient si on s'y fie trop largement de faire dépendre l'efficacité des régulations concernées de la bonne foi de l'entreprise compliante qui peut parfois cacher derrière une façade vertueuse des comportements de créative compliance s'éloignant plus ou moins fortement des règles qu'elle feint de respecter. Comme toutes les formes d'autorégulation elle éloigne une part du processus régulatoire du regard du régulateur public et cela peut parfois ouvrir la voie à des dérives comme la crise financière de 2007 2008 l'a bien montré. Les systèmes régulatoires doivent se préoccuper de mettre en place toutes les incitations possibles à prendre la conformité aux règles au sérieux. ».

1179 Merabet Samir, « La morale by design », *in* Frison-Roche Marie-Anne (dir.), *Les outils de la compliance*, éd. Dalloz, 2021, p. 294 ; Castets-Renard Céline, « Quels lien établir entre les USA et l'UE en matière de vie privée et protection des données personnelles ? », Dalloz IP/IT, 2016, p. 115 : « Ne nous leurrons cependant pas : l'opportunisme économique est le principal moteur de ce ralliement au droit européen, plutôt que de protéger les individus. ».

chimérique. Néanmoins, la perspective d'une sanction peut rendre à la compliance une certaine perspective d'effectivité.

2. La perspective indispensable d'une sanction pour les acteurs

425. La sanction comme outil de la compliance. La *compliance* est définie par ses objectifs mais également par ses outils. L'un des outils indispensables de la *compliance* est la perspective de la sanction[1180]. Il existe une temporalité avec la *compliance*, la logique de confiance se met en place *ex ante* par les opérateurs économiques et la sanction sera appliquée *ex post*[1181]. Les récents règlements ont augmenté considérablement le montant des amendes administratives. Lors de l'entrée en vigueur du Règlement sur la protection des données à caractère personnel, l'accent était mis sur les sanctions maximales pouvant aller jusqu'à 4% du chiffre d'affaires mondial[1182], l'augmentation des sanctions était déjà considérable. Désormais, le Règlement (UE) 2022/1925 du Parlement européen et du Conseil du 14 septembre 2022 relatif aux marchés contestables et équitables dans le secteur numérique prévoit que la sanction maximale peut s'élever jusqu'à 10% du chiffre d'affaires mondial total réalisé au niveau mondial au cours de l'exercice précédent pour les entreprises qualifiées de contrôleurs d'accès par la Commission européenne, et jusqu'à 20% en cas de récidive[1183]. Par ailleurs, la Commission peut adopter des décisions infligeant aux entreprises une astreinte jusqu'à concurrence de 5% de son chiffre

---

1180 Frison-Roche Marie-Anne, « Résoudre la contradiction entre "sanction" et "incitation" sous le feu du Droit de la compliance », *in* Frison-Roche Marie-Anne (dir.), *Les outils de la compliance*, éd. Dalloz, 2021, p. 91.

1181 Gerard Loic, « Les sanctions en cas de non-respect du RGPD : vers une plus grande effectivité de la protection des données à caractère personnel ? », *in* De Terwangne Cécile et Rosier Karen (dir.), *Le Règlement général sur la protection des données (RGPD / GDPR). Analyse approfondie*, éd. Larcier, 2018, pp. 641-652.

1182 Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), article 83 paragraphe 5 : « Les violations des dispositions suivantes font l'objet, conformément au paragraphe 2, d'amendes administratives pouvant s'élever jusqu'à 20 000 000 EUR ou, dans le cas d'une entreprise, jusqu'à 4 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu (…) ».

1183 Règlement (UE) 2022/1925 du Parlement européen et du Conseil du 14 septembre 2022 relatif aux marchés contestables et équitables dans le secteur numérique (règlement sur les marchés numériques), article 30 : « Dans la décision constatant un non-respect, la Commission peut infliger à un contrôleur d'accès des amendes jusqu'à concurrence de 10 % de son chiffre d'affaires total réalisé au niveau mondial au cours de l'exercice précédent lorsqu'elle constate que le contrôleur d'accès, volontairement ou par négligence, ne respecte pas (…) ».

d'affaires journalier moyen réalisé au niveau mondial au cours de l'année précédente par jour[1184]. La logique de *compliance* est alors renforcée par la perspective d'une sanction très élevée. L'augmentation des sanctions nous semble bénéfique, même si le montant des sanctions est toujours dérisoire pour ces acteurs du numérique : ils gagnent davantage à ne pas respecter les normes et à payer les amendes plutôt que l'inverse.

426. Appréciation du comportement. De surcroît, le respect du droit souple par l'analyse comportementale peut également être pris en compte pour l'évaluation de la sanction[1185]. En effet - dans le Règlement (UE) 2022/2065 du 19 octobre 2022 du Parlement européen et du Conseil relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (DSA) par exemple -, le code de conduite n'est plus un simple instrument de droit souple, il devient un instrument concret permettant de vérifier l'application du règlement sur les services numériques par les plateformes. Lors d'un litige, le juge pourra apprécier le degré de responsabilité en fonction du respect des divers codes adhérés. Le code de conduite devient un outil contraignant, dans la mesure où les plateformes s'exposent à des amendes pouvant aller jusqu'à 6% de leur chiffre d'affaires mondial[1186]. *In fine,* la norme de droit souple devient un « standard opportun » pour juger du caractère fautif de l'opérateur économique[1187]. Les acteurs qui ne sont pas qualifiés de très grande plateforme pourront adhérer aux engagements de leur choix. Pour les très grandes plateformes, autrement dit les principaux acteurs du numérique, le degré de liberté dans l'adhésion de la *soft law* tend à s'amoindrir au fil des normes[1188].

1184 *Ibid*., article 31.

1185 Bertrand Brunessen et Sirinelli Jean, *op. cit*.

1186 Règlement (UE) 2022/2065 du 19 octobre 2022 du Parlement européen et du Conseil relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (règlement sur les services numériques), article 52 paragraphe 3 : « Les États membres veillent à ce que le montant maximal des amendes qui peuvent être imposées pour non-respect d'une obligation établie dans le présent règlement représente 6 % du chiffre d'affaires mondial annuel du fournisseur de services intermédiaires concerné réalisé au cours de l'exercice précédent. Les États membres veillent à ce que le montant maximal de l'amende qui peut être imposée pour la fourniture d'informations inexactes, incomplètes ou trompeuses, l'absence de réponse ou la non-rectification d'informations inexactes, incomplètes ou trompeuses et le manquement à l'obligation de se soumettre à une inspection représente 1 % des revenus ou du chiffre d'affaires mondial annuels du fournisseur de services intermédiaires concerné ou de la personne concernée de l'exercice précédent. ».

1187 Deumier Pascale, « Quand le droit souple rencontre le juge dur », RTD civ, 2016, 571.

1188 Marti Gaëlle, « Les instruments normatifs de la politique du numérique », *in* Bertrand Brunessen (dir.), *La politique européenne du numérique*, éd. Bruylant, 2023, p. 238.

Les pouvoirs d'édiction de normes par les autorités administratives indépendantes font toutefois l'objet d'un contrôle par le juge. Le juge devient l'acteur principal pour garantir une cohérence dans le système en réseau.

B) L'indispensable contrôle du juge pour la cohérence du système

427. Le juge garant de la cohérence du système. Le maintien d'un certain ordre implique la présence du juge comme garant de la cohérence du système. Pour ce faire, le juge peut contrôler tant les actes des autorités administratives indépendantes (1) que les sanctions de ces autorités (2).

1. Le contrôle des actes des autorités administratives indépendantes

428. Confirmation de la validité d'un acte de droit souple. En 2019, le Conseil d'État a ouvert la voie du recours pour excès de pouvoir des actes de droit souple émis par la Commission nationale de l'informatique et des libertés[1189]. Dès lors que l'acte en question produit des effets considérables ou notables sur les personnes concernées, les actes peuvent faire l'objet d'un examen de légalité par le Conseil d'État, à l'instar des actes de droit dur. En l'espèce, il s'agissait de lignes directrices au sujet des *cookies*. La Commission nationale de l'informatique et des libertés avait abrogé une recommandation de 2013 sur les *cookies*, désormais en contradiction avec les lignes du RGPD. En effet, la recommandation admettait la possibilité d'un consentement « mou »[1190] : l'autorité de régulation a donc émis une feuille de route afin de migrer vers un système de consentement explicite. La « Quadrature du Net » et « Caliopen » ont contesté le document de « droit souple » de la Commission nationale de l'informatique et des libertés devant le Conseil d'État, aux motifs que la Commission nationale de l'informatique et des libertés aurait surpassé ses compétences. Le Conseil d'État a rejeté la requête, estimant que l'impact de la feuille de route n'était pas important sur les droits des citoyens[1191].

1189 Coupez François, Péronne Géraldine, « Consentement aux cookies : quelle est la bonne recette ? », Dalloz IP/IT, 2020, 189.

1190 Zolynski Célia, Maxwell Winston, « Protection des données personnelles », Recueil Dalloz, 2020, n°22, p. 1262.

1191 Conseil d'État, n° 433069, 16 octobre 2019, sur le recours pour excès de pouvoir introduit par la Quadrature du Net et Caliopen contre la délibération de la CNIL n° 2019-093 du 4 juillet 2019 portant adoption de lignes directrices.

Le Conseil d'État justifie de manière aisée sa décision au regard des négociations tardives sur la directive e-Privacy ainsi que sur l'incertitude prégnante des règles relatives aux cookies[1192]. Le rapporteur public dans son rapport confirme le fait que « tout le monde sait ce qu'il ne faut pas faire - assimiler poursuite de la navigation et consentement aux *cookies* -, mais personne ne sait exactement et concrètement ce qu'il faut faire.[1193] ». Le climat d'incertitude au sujet du consentement sur les *cookies* profite aux acteurs du numérique. Dans sa décision du 16 octobre 2019, le Conseil d'État relève que la Commission nationale de l'informatique et libertés ne peut être regardée comme ayant commis une erreur manifeste d'appréciation en retenant de telles orientations pour l'exercice de ses pouvoirs et rejette le recours formé par la Quadrature du Net et Caliopen. Ainsi, le juge rétablit une cohérence entre les normes en réseau et établit un cadre temporaire pour les *cookies* en attendant les évolutions.

429. Refus partiel de normativité d'un acte de droit souple. Dans un sens contraire, le Conseil d'État a partiellement censuré des lignes directrices de la Commission nationale de l'informatique et des libertés, toujours au sujet des *cookies*[1194]. L'autorité de régulation des données à caractère personnel avait adopté en juillet 2019 des lignes visant à préciser les règles applicables et les bonnes pratiques en matière de *cookies* depuis l'entrée en vigueur du règlement général sur la protection des données. Le Conseil d'État estime que la Commission nationale de l'informatique et des libertés ne pouvait pas, par un acte de droit souple, interdire de façon générale et absolue la pratique des *cookies*, c'est-à-dire le blocage de l'accès à un site web ou une application pour les personnes qui ne consentent pas au dépôt ou à la lecture de traceurs sur leur terminal[1195]. Pour le Conseil d'État, la Commission nationale de l'informatique et des libertés a excédé ce qu'elle pouvait légalement faire, dans le cadre d'un instrument de droit souple[1196]. Une telle interdiction ne peut résulter que d'un acte de « droit dur » émis par

[1192] 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).

[1193] Zolynski Célia, *op. cit.*

[1194] Conseil d'État, n° 434684, 19 juin 2020.

[1195] De Montecler Marie-Christine, « Les lignes directrices de la CNIL sur les cookies partiellement censurées », AJDA, 2020, 1264.

[1196] Conseil d'État, *op. cit*., point 10 : « D'autre part, la CNIL affirme, à ce même article 2, que la validité du consentement est soumise à la condition que la personne concernée ne subisse pas d'inconvénient majeur en cas d'absence ou de retrait de son consentement, un tel inconvénient majeur pouvant consister, selon elle, dans l'impossibilité d'accéder à un site internet, en raison de la pratique des "cookie walls". En déduisant pareille interdiction générale et absolue de la seule exigence d'un consentement libre, posé par le règlement du 27 avril 2016, la CNIL a excédé ce qu'elle peut légalement faire, dans le cadre d'un instrument de droit

une autorité ayant la compétence législative ou réglementaire[1197]. Néanmoins, le Conseil d'État rejette l'argument d'incompétence et rappelle que la Commission nationale de l'informatique et des libertés dispose du pouvoir de mettre en œuvre ses prérogatives par tout instrument qu'elle juge approprié, par exemple des lignes directrices[1198].

La présente décision démontre le rôle central du juge en matière de cohérence du système normatif. La Commission nationale de l'informatique et des libertés a continué ses travaux et a adopté des lignes directrices et une recommandation conformes à cet arrêt, validées le 4 mai 2020 par le Comité européen de la protection des données[1199].

430. Le contrôle du juge comme garant de la cohérence. Dans un cadre normatif en construction, le juge reste le garant d'une certaine cohérence du système. En effet, le juge garantit l'articulation entre les actes de droit souple et de droit dur et surtout, la frontière entre ces actes. Les autorités administratives indépendantes jouent avec les limites de leurs pouvoirs afin de développer des actes toujours plus divers[1200]. Parfois même, ces autorités « empiètent » sur les compétences d'autorités normatives ordinaires. La frontière incertaine de ces pouvoirs et donc de ces actes, rend extrêmement complexe une hiérarchie des actes par la suite. Dès 2001, le Conseil d'État évoquait déjà « l'ambiguïté magique » des actions de régulation de certaines autorités[1201]. En 2010, un rapport remis à l'Assemblée nationale reprochait aux autorités de régulation de développer leur production juridique « à la limite extrême de leurs

souple, édicté sur le fondement du 2° du I de l'article 8 de la loi du 6 janvier 1978 cité au point 3. Il s'ensuit que la délibération attaquée est, dans cette mesure, entachée d'illégalité. » ; Mallet-Poujol Nathalie, Droit des communications électroniques, Légipresse, 2021, 240.

1197 Bertrand Brunessen et Sirinelli Jean, « L'approche comportementale dans la régulation du numérique », *Entre art et technique : les dynamiques du droit: mélanges en l'honneur de Pierre Sirinelli*, éd. Dalloz, 2022, p. 591.

1198 Lebeau Marianna Denise et Balducci Alexandre, « Adoption des lignes directrices modificatives de la CNIL relatives aux cookies et traceurs à la suite de la décision du Conseil d'État du 19 juin 2020 : quelles conséquences en pratique ? », Dalloz IP/IT, 2021, 41.

1199 Commission nationale de l'informatique et des libertés, délibération n° 2020-091 du 17 septembre 2020 portant adoption de lignes directrices relatives à l'application de l'article 82 de la loi du 6 janvier 1978 modifiée aux opérations de lecture et écriture dans le terminal d'un utilisateur (notamment aux « cookies et autres traceurs ») et abrogeant la délibération n° 2019-093 du 4 juill. 2019 ; Commission nationale de l'informatique et des libertés, délibération n° 2020-092 du 17 sept. 2020 portant adoption d'une recommandation proposant des modalités pratiques de mise en conformité en cas de recours aux « cookies et autres traceurs ».

1200 Gaudemet Yves, « La régulation économique ou la dilution des normes », RDP 2017, p. 23.

1201 Conseil d'État, « Les autorités administratives indépendantes », Rapport public 2001, La Documentation française, 2001.

compétences[1202] ». Il est même parfois question de la légitimité des autorités administratives indépendantes et de la confusion des pouvoirs de ces autorités[1203]. En effet, les autorités sont chargées d'édicter des règles et d'en contrôler le respect. En réalité, il nous semble plus raisonnable de se pencher sur la légitimité des acteurs privés plutôt que celle des autorités administratives indépendantes. Par ailleurs, le contrôle du juge permet de maintenir la cohérence nécessaire au système en contrôlant les actes et les sanctions des autorités administratives indépendantes.

2. Le contrôle juridictionnel des sanctions des autorités administratives indépendantes

431. Contrôle des pouvoirs des AAI. Tout d'abord, avec la décision « HADOPI », le Conseil constitutionnel consacrait la liberté d'accéder aux services de communication en ligne comme partie de la liberté de communication et d'expression garantie par l'article 11 de la Déclaration des droits de l'Homme et du citoyen[1204]. En effet, la loi HADOPI avait pour mission principale de prévenir et de sanctionner le piratage. Pour ce faire, le texte adopté par le Parlement prévoyait, en cas de persistance, la suspension de l'abonnement à internet pour une durée allant de 3 mois à 1 an. Cette disposition a été censurée par le Conseil constitutionnel au motif qu'une autorité administrative ne dispose pas du pouvoir de prononcer une telle sanction, pouvoir incombant exclusivement au juge[1205]. Le juge constitutionnel est le garant du

---

[1202] Dosière René et Vanneste Christian, « Rapport d'information », déposé en application de l'article 146-3, alinéa 8, du Règlement par le comité d'évaluation et de contrôle des politiques publiques sur la mise en œuvre des conclusions du rapport d'information (n° 2925) du 28 octobre 2010 sur les autorités administratives indépendantes, décembre 2010, p. 380.

[1203] Haquet Arnaud, « Le pouvoir réglementaire des autorités administratives indépendantes », RDP, 2008, p. 393 : « L'attribution d'un pouvoir normatif à une autorité, qui n'est pas le légsilteur et qui n'est pas responsable devant lui, a toujours été perçue comme une forme de dépossession du pouvoir politique et comme une atteinte à l'unicité du pouvoir. L'octroi d'un pouvoir normatif à une autorité administrative, dont l'indépendance exprime sa non-politisation et son détachement de l'administration étatique, ne peut être vécu que comme une provocation. [...] Enfin, peut-on accepter qu'une autorité administrative soit chargée de sanctionner le non-respect des règles qu'elle édicte ? ».

[1204] Conseil constitutionnel, décision n° 2009-580 DC, 10 juin 2009.

[1205] Conseil constitutionnel, *op. cit*., point 16 : « Considérant que les pouvoirs de sanction institués par les dispositions critiquées habilitent la commission de protection des droits, qui n'est pas une juridiction, à restreindre ou à empêcher l'accès à internet de titulaires d'abonnement ainsi que des personnes qu'ils en font bénéficier ; que la compétence reconnue à cette autorité administrative n'est pas limitée à une catégorie particulière de personnes mais s'étend à la totalité de la population ; que ses pouvoirs peuvent conduire à restreindre l'exercice, par toute personne, de son droit de s'exprimer et de communiquer librement, notamment depuis son domicile ; que, dans ces conditions, eu égard à la nature de la liberté garantie par

contrôle de proportionnalité, en l'espèce des pouvoirs des autorités administratives indépendantes. Les pouvoirs de ces autorités sont certes évolutifs, il convient cependant de délimiter strictement leur pouvoir de sanction.

432. Contrôle des sanctions infligées par la CNIL. Par ailleurs, il existe un contrôle sur les sanctions pécuniaires prononcées par les autorités administratives indépendantes[1206]. Le Conseil d'État contrôle également le montant des sanctions prononcées par la Commission nationale de l'informatique et des libertés. À titre d'illustration, le 28 janvier 2022, le Conseil d'état a confirmé deux amendes d'un montant total de 100 millions d'euros infligées par l'autorité administrative indépendante à l'encontre de Google en décembre 2020[1207]. Toujours au sujet des *cookies*, la formation restreinte de la Commission nationale de l'informatique et des libertés avait sanctionné la société « Google LLC » d'une amende de 60 millions d'euros et la société « Google Ireland Limited » d'une amende de 40 millions d'euros pour avoir déposé des *cookies* publicitaires sur les ordinateurs d'utilisateurs du moteur de recherche « google.fr » sans consentement préalable ni information satisfaisante[1208]. Le Conseil d'État estime que le montant n'excède pas la limite prévue par la loi et qu'il est raisonnable au regard des bénéfices produits par les données collectées au moyen de *cookies* publicitaires par Google. Le montant de l'amende prononcée par l'autorité administrative indépendante est proportionné au regard de la position économique importante de Google, de la gravité du manquement et du grand nombre d'utilisateurs concernés[1209]. Ainsi, le Conseil d'État refuse - fort heureusement - d'annuler la sanction infligée à Google par la Commission nationale de l'informatique et des libertés. En effet, les acteurs du numérique sont d'ordinaire de mauvaise foi au sujet de leur argumentation[1210].

---

l'article 11 de la Déclaration de 1789, le législateur ne pouvait, quelles que soient les garanties encadrant le prononcé des sanctions, confier de tels pouvoirs à une autorité administrative dans le but de protéger les droits des titulaires du droit d'auteur et de droits voisins. ».

[1206] Autin Jean-Louis, « Le devenir des autorités administratives indépendantes », RFDA, 2010, 875.

[1207] Conseil d'État, 28 janvier 2022, n° 449209, publié au recueil Lebon.

[1208] Hardouin-Ayrinhac Marie-Lou, « Cookies publicitaires », La lettre juridique, 2 février 2022.

[1209] Cécile Crichton, « Cookies : sanction de Google par la CNIL confirmée », Dalloz IP/IT 2022, 62 ; points 21 à 27 de la décision.

[1210] Netter Emmanuel, « "Refuser tous les cookies ". Espoirs et mirages d'une régulation par les boutons », Dalloz IP/IT 2022 p. 392 : « Ni Google ni Facebook ne pouvaient sérieusement prétendre qu'ils ignoraient que la CNIL s'apprêtait à les poursuivre. Ses lignes directrices, ses communiqués de presse étaient sans ambiguïté à cet égard. S'agissant de Google, un courrier du secrétaire général en date de février 2021 s'était même montré particulièrement explicite. Juridiquement, l'argumentation de la CNIL est donc sans faiblesse. ».

433. Conclusion de la section. Pendant les dernières années, les pouvoirs des autorités de contrôle se sont diversifiés et intensifiés afin de s'adapter aux enjeux. Le renforcement des pouvoirs de contrôle et de sanction de ces autorités administratives indépendantes est légitime et surtout, nécessaire. Afin de maintenir une certaine cohérence dans le système, les autorités de régulation nécessitent une articulation souple entre elles. En effet, il existe tout un système de régulation en réseau de ces autorités. Les secteurs s'entrecroisent et exigent une interrégulation entre les différentes autorités. Pour ce faire, elles coopèrent dans le dessein de réguler de manière efficiente les secteurs, au niveau national et au niveau européen.

Au niveau des autorités administratives indépendantes, il existe une articulation interne, permettant de garantir une application efficace de leurs prérogatives. L'articulation des autorités administratives indépendantes est indispensable afin de garantir l'effectivité du cadre normatif et prononcer des sanctions dissuasives. Au niveau des entreprises, un système de *compliance* s'est progressivement instauré. Les autorités de régulation conservent une place déterminante en élaborant les normes de droit souple utilisées en partie dans la *compliance.* La *compliance* utilise toute la gamme de normativité afin de ne pas brider l'innovation dans un premier temps. Les acteurs sont responsabilisés par l'incitation plutôt que par la contrainte. Ils doivent respecter un ensemble de normes afin d'atteindre des objectifs ciblés.

Pour le droit des données, l'objectif est la protection des données à caractère personnel des utilisateurs. En réalité, l'internalisation des normes par les acteurs est utopique. L'objectif des acteurs du numérique est exclusivement mercantile. Il devient illusoire d'instaurer des mécanismes de *compliance* pour et par des entreprises privées. Avec l'internalisation des normes par les acteurs du numérique, ils profitent de leur connaissance technique afin de contourner les normes faussement appliquées. Il reste la perspective d'une sanction afin de les contraindre à appliquer les normes en amont. En réalité, les sanctions sont rarement dissuasives au regard de leur chiffre d'affaires. À nouveau, la diversité des outils de régulation et des instances de régulation profitent à ces acteurs, censés être les protagonistes du système régulation.

In fine, il existe aujourd'hui un « écosystème de multirégulation » intégrant les autorités administratives indépendantes et les opérateurs économiques dans un système de réseau de

normes[1211]. Il n'existe plus une articulation au sens stricte mais une balance des intérêts effectuée par le juge. Ainsi, le juge reste le gardien en cas de défaillance ou d'abus de pouvoirs, que ce soit pour les autorités administratives indépendantes comme pour les acteurs privés[1212].

[1211] Vivant Michel, « Internet et les nouveaux services », Rapport de synthèse du sommet mondial des régulateurs, Paris, 1999.
[1212] Quéméner Myriam, « Le Magistrat, régulateur ponctuel, régulateur final », *in* Frison-Roche Marie-Anne (dir.), *Internet, espace d'interrégulation*, éd. Dalloz, 2016, p. 180.

Section 2 : L'articulation superficielle des mécanismes de protection des données à caractère personnel

434. Construction d'un droit fondamental. Le droit des données s'est construit autour du règlement sur la protection des données à caractère personnel. Un droit fondamental a progressivement émergé afin de protéger effectivement les données à caractère personnel des personnes concernées. La protection des données à caractère personnel se retrouve au sommet d'une certaine hiérarchie des normes concernant le droit des données. Par conséquent, toutes les législations doivent respecter les obligations du règlement. Pour les acteurs du numérique, qu'importe le secteur ou le domaine, dès lors qu'ils traitent des données à caractère personnel, ils doivent respecter le règlement sur la protection des données. Ainsi, l'ensemble du droit des données serait soumis au respect de la protection des données à caractère personnel.

435. Superficialité de la prévalence. En pratique, la protection annoncée des données à caractère personnel s'avère quelque peu superficielle. La superficialité peut se définir comme « une pensée qui reste à la surface des choses, qui manque de profondeur[1213]. ». La garantie de la prévalence de la protection des données à caractère personnel nous semble pouvoir être qualifiée de superficielle avec le développement des technologies émergentes et des nouvelles pratiques (I). Afin de tempérer le caractère superficiel de cette protection, les autorités administratives indépendantes ainsi que la Cour de justice n'hésitent pas à avoir une interprétation extensive des principes du règlement afin de s'adapter réellement aux usages des données. Pour ce faire, le domaine de protection est étendu de façon délibérée par les acteurs de la réglementation et de la régulation (II).

[1213] Définition Larousse, v° « Superficiel », point 3.

I. La superficielle prévalence de la protection des données à caractère personnel à travers les réglementations

436. Annonce de plan. L'ensemble des règlements concernant les données prennent en compte l'éventuel conflit de lois entre les règlements concernant l'ouverture des données et les objectifs de protection des données à caractère personnel. Sans exception, les divers règlements doivent s'appliquer sans préjudice du règlement sur la protection des données, conférant une primauté incontestable du RGPD dans la hiérarchie des normes (A). En réalité, la primauté est amplement contestable au regard des nouveaux usages numériques (B).

A) La prévalence incontestable du RGPD dans la hiérarchie des normes des données

437. Protection des individus. Le droit des données à caractère personnel s'est construit progressivement depuis la fin des années 1970. Avec le développement des technologies émergentes, les risques pour les individus se sont accentués. L'aspiration croissante de protection des individus a peu à peu conféré au droit des données à caractère personnel un caractère fondamental (1). Grâce à la consécration de cette protection en un droit fondamental, la primauté des données à caractère personnel s'illustre également en cas de conflit de normes (2).

1. La prévalence fondamentale de la protection des données à caractère personnel

438. Un droit fondamental. La Charte des droits fondamentaux de l'Union européenne est devenue l'instrument de référence en matière de protection des droits[1214]. Depuis l'entrée en vigueur du traité de Lisbonne, la Charte bénéficie d'une valeur juridique équivalente à celle des traités[1215]. Principalement, c'est un instrument qui participe au renforcement des droits fondamentaux dans l'Union à la lumière de l'évolution de la société et des développements technologiques[1216], jouant un rôle essentiel dans la protection des données à caractère personnel[1217]. En effet, l'article 8 de la Charte dispose que « toute personne a droit à la protection

[1214] Charte des droits fondamentaux de l'Union européenne, 2000, C 346/01.
[1215] Traité sur le fonctionnement de l'Union européenne, article 6.
[1216] Charte des droits fondamentaux de l'Union européenne précité, préambule, alinéa 4.
[1217] Douville Thibault, *Droit des données à caractère personnel*, éd. LGDJ, 2023, p. 28.

des données à caractère personnel la concernant[1218] ». La présence de l'article au sein de la Charte élève la protection des données à caractère personnel en un droit fondamental[1219]. Par conséquent, la Charte est dotée de la même force normative que le droit primaire[1220] et la place de la protection des données à caractère personnel dans la Charte fondamentale est - au-delà de l'aspect symbolique - indispensable pour la garantie des droits des individus[1221]. Il convient de rappeler que le Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données érige une véritable gouvernance de la donnée. En effet, le règlement protège les données à caractère personnel concernant une personne et non la personne elle-même[1222]. La distinction de protection entre les données à caractère personnel et la personne résulte de la prise en compte d'objectifs divergents, la protection et l'ouverture des données. Pour autant, le considérant premier du règlement rappelle que « la protection des personnes physiques à l'égard du traitement des données à caractère personnel est un droit fondamental[1223] ». La protection des données à caractère personnel est progressivement devenue un droit fondamental, se plaçant désormais « au frontispice de la hiérarchie des normes[1224] ».

[1218] Charte des droits fondamentaux de l'Union européenne, *op. cit*., article 8.1.

[1219] Ailincai Mihaela Anca, « Différents standards européens de protection des données ? À propos du droit de l'Union européenne et du droit du Conseil de l'Europe », *in* Bensamoun Alexandra et Bertrand Brunessen (dir.), *Le règlement général sur la protection des données, Aspects institutionnels et matériels*, éd. Mare & Martin, 2020, p.101.

[1220] Tinière Romain, « L'apport de la Charte des droits fondamentaux à la protection des données personnelles dans l'Union européenne », RAE, n° 2018/1, p. 30.

[1221] Benabou Valérie-Laure « La Cour de justice, gardienne d'une "souveraineté européenne" sur les données », RAE, 2018/1, p. 22 : « Sans avoir besoin d'un acquiescement législatif, la Cour énonce, en convoquant l'instrument prétorien des principes généraux du droit, le rattachement de la protection des données à cette catégorie de règles dotées d'une force normative supérieure. Elle ne le fait pas dans une perspective seulement symbolique mais afin de trancher des litiges en respectant un équilibre des intérêts ayant une même intensité normative et donner ainsi à la protection des données à caractère personnel la possibilité d'être opposée avec une certaine autorité à d'autres règles concurrentes. ».

[1222] Tinière Romain, « Les données personnelles, source de nouveaux droits fondamentaux ? », *in* Bruguière Jean-Michel (dir.), *L'émergence d'un droit des données*, éd. Dalloz, 2023, p. 62.

[1223] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), considérant 1.

[1224] Castets-Renard Céline, « La protection des données personnelles dans les relations internes à l'Union européenne », Répertoire de droit européen, 5. Données personnelles et droit fondamental.

439. Article 16 du Traité sur le fonctionnement de l'Union européenne (TFUE). Par ailleurs, la primauté et surtout l'importance de la protection des données à caractère personnel s'illustrent par la création de l'article 16 du Traité sur le fonctionnement de l'Union européenne. En effet, il consacre le droit à toute personne « à la protection des données à caractère personnel le concernant[1225] ». L'institution de cet article constitue une base juridique propre pour l'adoption de règles en matière de données à caractère personnel. Ainsi, le Règlement sur la protection des données à caractère personnel, la directive 2016/680 et le règlement 2018/1725 ont été adoptés sur cette base juridique. La place « fondamentale » de la protection des données à caractère personnel dans le système est illustrée par sa priorité indéniable dans les divers règlements concernant les données. La protection des données à caractère personnel constitue un « prérequis » sur lequel doivent se conformer les nouvelles législations[1226].

2. La prévalence textuelle du règlement (UE) 2016/679

440. Hiérarchie des normes sur les données. L'ensemble de l'édifice sur la stratégie des données s'apprécie autour du règlement (UE) 2016/679 sur la protection des données à caractère personnel[1227]. Les règlements qui succèdent ont pour obligation de respecter la protection des données à caractère personnel afin de garantir une cohérence dans le cadre normatif européen[1228]. Ainsi, pour tous les règlements concernant les données, la priorité de protection des données à caractère personnel est incontestable. Il existe alors un semblant de hiérarchie entre les données, donnant la primauté aux données à caractère personnel dans l'ensemble des règlements.

441. Pour l'ouverture des données. En effet, le Règlement (UE) 2018/1807 sur le libre flux des données à caractère non personnel prévoit que « lorsque les données à caractère personnel et les données à caractère non personnel d'un ensemble sont inextricablement liées, le présent

---

[1225] Traité sur le fonctionnement de l'Union européenne (TFUE), article 16 paragraphe 1.

[1226] Comité européen de la protection des données (CEPD), avis conjoint, p. 8 : « Le droit de l'Union applicable en la matière, et en particulier le règlement (UE) 2016/679 (règlement général sur la protection des données, RGPD), est considéré comme étant un prérequis sur lequel de nouvelles propositions législatives peuvent s'appuyer sans affecter les dispositions existantes pertinentes ou interférer avec celles-ci, y compris lorsqu'il s'agit de la compétence des autorités de contrôle et d'autres aspects liés à la gouvernance. ».

[1227] Huttner Liane, « Mesurer l'effectivité du RGPD », RAE, n° 2023/4, pp. 951-961.

[1228] Métallinos Nathalie, « L'évolution du droit européen en matière de protection des données à caractère personnel », L'observatoire de Bruxelles, n° 93, 2013, p. 17.

règlement est sans préjudice de l'application du règlement (UE) 2016/679[1229] ». Dès 2018, le règlement sur le libre flux des données à caractère non personnel prévoit la priorité des données à caractère personnel sur un ensemble de données. Pour les données publiques, la Directive (UE) 2019/1024 du Parlement européen et du Conseil du 20 juin 2019 concernant les données ouvertes et la réutilisation des informations du secteur public prévoit également que « la présente directive est sans préjudice des dispositions du droit de l'Union et du droit national sur la protection des données à caractère personnel, en particulier le règlement (UE) 2016/679 et la directive 2002/58/CE, ainsi que des dispositions correspondantes du droit national[1230] ». L'objectif d'*open data* est logiquement impacté par la protection des données à caractère personnel. Afin d'ouvrir davantage les données, le Règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données (DGA) et le Règlement (UE) 2023/2854 du Parlement européen et du Conseil du 13 décembre 2023 concernant des règles harmonisées portant sur l'équité de l'accès aux données et de l'utilisation des données (DA) laissent davantage de flexibilité quant aux données à caractère personnel. Néanmoins, les règlements précités évoquent constamment la priorité de la protection des données à caractère personnel sur l'ensemble des données.

442. Pour le DGA. La protection des données à caractère personnel a été l'un des enjeux principaux lors des négociations du Règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données (règlement sur la gouvernance des données). La version initiale proposée comportait des incohérences avec le règlement sur la protection des données[1231]. Finalement, un consensus sur la priorité du droit à la protection des données à caractère personnel a émergé. Le règlement sur la gouvernance des données a donc été adapté aux règles, définitions et principes du règlement européen sur la protection des données à caractère personnel[1232]. Par exemple, les autorités de contrôle du

[1229] Règlement (UE) 2018/1807 établissant un cadre applicable au libre flux des données à caractère non personnel dans l'Union européenne, article 2, 2 : « Dans le cas d'un ensemble de données composé à la fois de données à caractère personnel et de données à caractère non personnel, le présent règlement s'applique aux données de l'ensemble à caractère non personnel. Lorsque les données à caractère personnel et les données à caractère non personnel d'un ensemble sont inextricablement liées, le présent règlement est sans préjudice de l'application du règlement (UE) 2016/679. ».

[1230] Directive (UE) 2019/1024 du Parlement européen et du Conseil du 20 juin 2019 concernant les données ouvertes et la réutilisation des informations du secteur public, article 2, point 4.

[1231] EDPB et CEPD, Avis conjoint sur la proposition du règlement sur la gouvernance européenne des données (acte sur la gouvernance des données), n° 03/2021, 10 mars 2021.

[1232] Petel Antoine, « L'Acte sur la gouvernance des données. L'Union européenne dévoile le premier pilier du marché européen des données », La Semaine juridique. Édition générale, 2022.

RGPD ne peuvent pas voir leurs prérogatives et compétences diminuées au profit de celles chargées de mettre en œuvre le règlement sur la gouvernance des données. Dès les considérants, le règlement prévoit qu'il est « sans préjudice du règlement (UE) 2016/679 du Parlement européen et du Conseil[1233] » rappelant qu'étant donné que les données à caractère personnel « relèvent du champ d'application de certains éléments du règlement, les mesures sont conçues de manière à respecter pleinement les dispositions législatives en matière de protection des données et à renforcer en pratique le contrôle que les personnes physiques exercent sur les données qu'elles génèrent[1234]». Le considérant 46 précise que : « le présent règlement respecte les droits fondamentaux et observe les principes reconnus en particulier par la charte des droits fondamentaux de l'Union européenne, notamment le respect de la vie privée, la protection des données à caractère personnel ». Néanmoins, il est possible de souligner l'absence de référence à l'article 16 du TFUE comme fondement du règlement[1235]. Au contraire, cela marque la volonté de l'Union européenne d'ouvrir davantage les données dans un objectif de marché unique dynamique.

443. Pour le DA. Pour le Règlement (UE) 2023/2854 du Parlement européen et du Conseil du 13 décembre 2023 concernant des règles harmonisées portant sur l'équité de l'accès aux données et de l'utilisation des données (règlement sur les données), ce dernier souligne l'exigence de cohérence du cadre normatif en commençant la proposition par rappeler que « la présente proposition est cohérente avec les règles existantes concernant le traitement des données à caractère personnel (notamment le règlement général sur la protection des données (RGPD)[1236]. ». Le règlement rappelle la nature fondamentale de la protection des données à caractère personnel dans son considérant 7[1237]. Par ailleurs, le règlement sur les données précise

1233 Règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données (règlement sur la gouvernance des données), considérant 3.

1234 Règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données (règlement sur la gouvernance des données), motifs p. 7.

1235 Douville Thibault et Netter Emmanuel, « Présentation critique du Data governance act », RTD com. 2022. 561.

1236 Proposition de règlement relatif à des règles harmonisées sur un accès équitable aux données et sur leur utilisation (règlement sur les données), COM(2022) 68 final, p. 4.

1237 *Ibid*., considérant 7 : « Le droit fondamental à la protection des données à caractère personnel est garanti notamment par le règlement (UE) 2016/679 et le règlement (UE) 2018/1725. La directive 2002/58/CE protège, quant à elle, la vie privée et la confidentialité des communications en prévoyant notamment des conditions régissant tout stockage de données à caractère personnel et de données à caractère non personnel dans un équipement terminal et l'accès aux unes et aux autres à partir dudit équipement. Ces instruments servent de base à un traitement pérenne et responsable des données, y compris lorsque les ensembles de données contiennent un mélange de données à caractère personnel et de données à caractère non personnel.

que « lorsqu'il est strictement nécessaire d'inclure des données à caractère personnel dans les données mises à la disposition d'un organisme du secteur public ou d'une institution, d'un organe ou d'un organisme de l'Union, les règles applicables en matière de protection des données à caractère personnel devraient être respectées et la mise à disposition des données et leur utilisation ultérieure devraient s'accompagner de garanties pour les droits et intérêts des personnes concernées par ces données[1238]. ».

444. Pour le DMA et DSA. Pour le règlement (UE) 2022/1925 sur les marchés numériques, le considérant 12 dispose que : « le présent règlement devrait également s'appliquer sans préjudice des règles qui découlent d'autres actes régissant certains aspects de la fourniture de services couverts par le présent règlement, en particulier les règlements (UE) 2016/679 et (UE) 2019/1150[1239] » et rappelle que « le présent règlement est sans préjudice du règlement (UE) 2016/679, y compris son cadre d'application, qui reste pleinement applicable en ce qui concerne toute réclamation introduite par des personnes concernées en rapport avec une infraction aux droits que leur confère ledit règlement[1240]. ». Concernant le règlement 2022/2065 sur les services numériques, le règlement est applicable « sans préjudice du droit de l'Union en matière de protection des données à caractère personnel, en particulier le règlement (UE) 2016/679[1241] », en précisant que « les exigences du présent règlement concernant la fourniture d'informations relatives à la publicité sont sans préjudice de l'application des dispositions pertinentes du règlement (UE) 2016/679, en particulier celles relatives au droit d'opposition, à la prise de décision individuelle automatisée, y compris le profilage, et en particulier à la nécessité d'obtenir le consentement de la personne concernée avant de traiter des données à caractère personnel à des fins de publicité ciblée[1242]. ».

Le présent règlement complète, sans y porter atteinte, les dispositions de droit de l'Union relatives à la protection des données et à la vie privée, en particulier le règlement (UE) 2016/679 et la directive 2002/58/CE. Aucune disposition du présent règlement ne devrait être appliquée ou interprétée de manière à réduire ou à limiter le droit à la protection des données à caractère personnel ou le droit à la vie privée et à la confidentialité des communications. ».

[1238] *Ibid*., considérant 64.

[1239] Règlement (UE) 2022/1925 du Parlement européen et du Conseil du 14 septembre 2022 relatif aux marchés contestables et équitables dans le secteur numérique (règlement sur les marchés numériques), considérant 12.

[1240] *Ibid*., considérant 37.

[1241] Règlement (UE) 2022/2065 du 19 octobre 2022 du Parlement européen et du Conseil relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (règlement sur les services numériques, considérant 10.

[1242] *Ibid*., considérant 68.

445. Pour l'intelligence artificielle. Au sujet du règlement 2024/1689 sur l'intelligence artificielle, ce dernier précise que les règles harmonisées prévues par le règlement devraient s'appliquer dans tous les secteurs et « être sans préjudice du droit de l'Union en vigueur, en particulier en ce qui concerne la protection des données[1243] », « le droit au respect de la vie privée et la protection des données à caractère personnel doit être garanti tout au long du cycle de vie du système d'intelligence artificielle. À cet égard, les principes de minimisation et de protection des données dès la conception et par défaut, tels qu'énoncés dans le droit de l'Union sur la protection des données, sont applicables lorsque des données à caractère personnel sont traitées[1244]. ». Concernant son champ d'application, le règlement rappelle que « le droit de l'Union en matière de protection des données à caractère personnel, de respect de la vie privée et de confidentialité des communications s'applique aux données à caractère personnel traitées en lien avec les droits et obligations énoncés dans le présent règlement[1245]. ». En effet, le champ d'application du règlement sur l'intelligence artificielle paraît plus large que celui du Règlement sur la protection des données à caractère personnel. Le simple fait que les résultats produits par un système d'intelligence artificielle soient utilisés dans l'Union rend applicable le règlement, allant plus loin que le critère de focalisation du RGPD[1246].

Incontestablement, les textes donnent la priorité au Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données. En réalité, la priorité de la protection des données à caractère personnel nous semble superficielle. Avec le développement des technologies émergentes et particulièrement l'intelligence artificielle, la primauté du texte s'amenuise.

B) La prévalence contestable du RGPD en pratique

[1243] Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle (règlement sur l'intelligence artificielle), considérant 9.
[1244] *Ibid.*, considérant 69.
[1245] *Ibid*., article 2 point 7.
[1246] Debet Anne, « Intelligence artificielle et droit des données à caractère personnel », *in* Bensamoun Alexandra et Loiseau Grégoire (dir.), *Droit de l'intelligence artificielle*, éd. LGDJ, 2022, p. 325.

446. Identification de la règle applicable. La multiplicité des règlements a pour conséquence le chevauchement de certaines notions. Par ailleurs, l'identification des règles spéciales et générales est parfois délicate en matière de données à caractère personnel (1). Surtout, le bouleversement des usages rend la primauté du règlement sur la protection des données à caractère personnel particulièrement contestable (2).

1. Le chevauchement des régimes

447. Prévalence d'articulation. Théoriquement, la prévalence de la protection des données à caractère personnel est incontestable. En réalité, il existe plusieurs règles spéciales qui interagissent avec le corpus sur les données à caractère personnel. Par exemple, les objectifs de la directive e-Privacy se cumulent avec les objectifs du règlement sur la protection des données à caractère personnel. En effet, la directive 2002/58/CE dite directive e-Privacy - révisée une première fois en 2009 - devait à nouveau être révisée et entrée en vigueur avec le RGPD. Les modifications de la révision entrainant des barrières pour le modèle économique des acteurs du numérique, la directive n'est toujours pas adoptée. Ainsi, le régime des cookies est régi par la directive 2002/58/CE et par certaines règles du RGPD, instituant un « ménage à trois délicat[1247] ». L'application combinée des règles au sujet de la publicité ciblée était complexe, notamment par rapport à la diversité et la multitude d'acteurs du secteur et de l'intrication des nombreux flux de données entre les divers acteurs[1248]. Il était question de savoir si l'existence de règles spéciales écartait l'application des règles prévues par le règlement européen[1249].

L'incertitude concernant les régimes applicables demeure en permanence favorable aux acteurs du numérique[1250]. Ils vont pouvoir altérer leurs responsabilités avec des développements sur les

[1247] Dubois Lorette et Gaullier Florence, « Publicité ciblée en ligne, protection des données à caractère personnel et ePrivacy : un ménage à trois délicat », Legicom, n° 59, 2017, pp. 69-102.
[1248] *Ibid*.
[1249] Danis-Fatôme Anne, « Cookies et autres traceurs : Articulation des sources, compétence de la CNIL et manquements aux règles applicables aux traceurs à des fins publicitaires », CCE, 2021.
[1250] Metallinos Nathalie, « Lignes directrices du G29 sur le consentement », CCE, 2019 : « Reste que le durcissement attendu des règles relatives au consentement liées à l'utilisation de cookies à des fins de ciblage publicitaire risque de détourner les acteurs vers des solutions pouvant paraître plus intrusives, et qui ne reposent pas sur le traitement de données pseudonymes, à savoir l'usage d'identifiants marketing uniques mis en œuvre par les acteurs tels que Microsoft ou Google qui sont directement rattachés à l'utilisateur et non seulement au terminal comme les cookies. Ce qui laisse perplexe sur la capacité du nouveau cadre européen sur la protection des données de tenir ses promesses face aux modèles économiques développés par les acteurs de l'économie numérique. ».

interprétations textuelles. Fort heureusement, la Commission nationale de l'informatique et des libertés a partagé ses lumières en 2020 sur l'articulation de ces deux sources. Au regard du principe d'articulation entre les règles générales et les règles spéciales, la Commission nationale de l'informatique et des libertés rappelle que le droit spécial écarte le droit général[1251]. L'autorité de régulation permet alors de rétablir une certaine cohérence entre les règles. En réalité, les acteurs du numérique arrivent encore à contourner les règles en matière de *cookies*.

448. Divergences ou chevauchements des notions. Par ailleurs, la multiplicité de régime et de notions peut parfois entrainer des difficultés d'articulation entre les régimes. Par exemple, la directive e-Privacy ignore la qualification de données à caractère personnel alors que les données de communications électroniques sont manifestement des données à caractère personnel[1252]. En réalité, les données de communications électroniques peuvent révéler des secrets d'affaires ou autres informations sensibles ayant une valeur économique[1253]. Par ailleurs, avec la multiplication des règlements entrés en vigueur, certains acteurs vont être confrontés à une diversité de qualification et par conséquent, de régime. Une plateforme peut être à la fois un « hébergeur » au sens de la directive 2000/31 du 8 juin 2000, un « responsable de traitement » au sens du RGPD, des « prestataires de services d'intermédiation en ligne » selon le règlement P2B ou encore un « fournisseur de services de partage de contenus » en ligne dans la DAMUN[1254]. De surcroît, avec l'entrée en vigueur du règlement sur l'intelligence artificielle, un fournisseur de système d'intelligence artificielle pourra être qualifié de responsable de traitement pour les données à caractère personnel utilisées pendant la phase d'entraînement. En revanche, la qualification pourra être modifiée dans le temps pour les étapes ultérieures de l'utilisation du système d'intelligence artificielle[1255]. La modification de qualification entraîne des obligations divergentes. À nouveau, avec l'expérience et des interprétations normatives

[1251] Commission nationale de l'informatique et des libertés, délibération n° SAN-2020-012, 7 décembre 2020 : « de même, il ressort du considérant 173 du RGPD que ce texte prévoit explicitement n'être pas applicable aux traitements de données à caractère personnel soumis à des obligations spécifiques ayant le même objectif énoncé dans la directive 2002/58/CE du Parlement européen et du Conseil, y compris les obligations incombant au responsable de traitement et les droits des personnes physiques ».

[1252] Michéa Frédérique, « L'appréhension de la donnée en droit de l'Union européenne », *in* Nevejeans Nathalie (dir.), *Données et technologies numériques*, éd. Mare et Martin, 2021, p. 32.

[1253] Castets-Renard Céline, *Droit du marché unique numérique et intelligence artificielle,* éd. Bruylant, 2020, p. 295.

[1254] Martial-Braz Nathalie, « La transdisciplinarité du droit numérique », *Mélanges en l'honneur de Michel Vivant. Penser le droit de la pensée*, éd. Dalloz, 2020, p. 853.

[1255] Padova Yann, « l'IA Act est-il réconciliable avec le RGPD et comment ? », Revue Lamy Droit de l'Immatériel, n° 209, 2023.

incertaines, les acteurs du numérique pourront choisir la qualification la plus favorable afin de perpétuer leurs usages.

2. Le bouleversement des usages

449. Développement de l'intelligence artificielle. En réalité, les régimes juridiques sont bouleversés par les usages du numérique, et particulièrement avec l'intelligence artificielle[1256]. Malgré l'importance théorique de la protection des données à caractère personnel dans le conflit des normes, la prévalence de la protection n'est pas nécessairement respectée[1257]. Néanmoins, la protection des données à caractère personnel ne doit pas être « sacrifiée » au nom de l'innovation[1258]. L'intelligence artificielle repose sur l'usage massif et mouvant de données et ignore la distinction entre donnée à caractère personnel et donnée à caractère non personnel[1259]. Dans cette hypothèse, le principe de finalité - principe central de la protection des données à caractère personnel - ne pourra être déterminé qu'*a posteriori.* Les protections instaurées dans le règlement sur l'intelligence artificielle paraissent dès à présent insuffisantes au regard des technologies émergentes[1260]. Plusieurs techniques d'intelligence artificielle devraient être purement et simplement interdites au regard des risques sur le droit fondamental de protection des données à caractère personnel[1261]. Par ailleurs, les fournisseurs de système d'intelligence artificielle vont rencontrer des difficultés pour satisfaire à leurs obligations. Lorsque le règlement prévoit un droit à l'explication de la prise de décision individuelle pour les décisions entièrement automatisées, l'entreprise utilisatrice ne sera pas forcément en mesure de fournir une telle explication au regard de l'opacité des pratiques et du système technique en lui-même.

1256 Favreau Amélie, « Données de santé : vers l'émergence d'un droit spécial ? », *in* Bruguière Jean-Michel (dir.), *L'émergence d'un droit des données*, éd. Dalloz, 2023, p 172.

1257 Chardeaux Marie-Alice, « Réseaux sociaux et données personnelles : avons-nous pris la mesure des menaces qui nous guettent ? », CCE, n° 1, janvier 2021, p. 4 : « En second lieu, les remèdes actuels sont insuffisants car les réseaux sociaux font peu de cas de la réglementation sur les données personnelles. ».

1258 Castets-Renard Céline, « Nouvelles technologies et droit européen : quel droit face à l'intelligence artificielle ? », *in* Sylvie Peyrou-Bartoll (dir.), *Nouvelles technologies et droit européen : quel droit face à la disruption numérique ?*, éd. Mare et Martin, 2022, p. 13.

1259 Bensamoun Alexandra et Loiseau Grégoire, « L'intelligence artificielle : faut-il légiférer ? », D., 2017, 581.

1260 Betty Jeulin, « Amendement de l'Artificial Intelligence Act : la théorie confrontée à la pratique », Dalloz Actualité, 14 juin 2023.

1261 Colpas Anna, « L'approche européenne de l'Intelligence Artificielle : brève analyse de l'interaction avec le droit à la vie privée et à la protection des données à caractère personnel », L'observateur de Bruxelles, 2021/4, n° 126, p. 23 ; Féral-Schuhl Christiane et Sinibaldi Justine, « Le RGPD challengé par l'intelligence artificielle », L'observateur de Bruxelles, 2023/2, n° 132, p. 28.

450. Développement de l'ouverture des données pour l'intelligence artificielle. En outre, l'objectif des récents règlements tels que le règlement sur les données (DA) ou sur la gouvernance des données (DGA) est prioritairement l'ouverture des données. L'accès aux données est primordial pour le développement de l'intelligence artificielle et, est devenu la direction prise par la Commission européenne. La prévalence de la protection des données à caractère personnel devient quelque peu théorique. En effet, les conceptions du règlement sur la protection des données à caractère personnel et du règlement sur l'intelligence artificielle sont divergentes. Lorsque le RGPD repose sur une approche personnaliste, le règlement sur l'intelligence artificielle repose sur une approche par les risques, inspirée des réglementations en matière de sécurité des produits[1262]. De surcroît, lors de l'analyse du règlement sur la gouvernance des données, le caractère altruiste de la donnée détourne l'obligation de finalité de la donnée personnelle pour lui reconnaître une finalité d'utilité générale et de développement de l'innovation[1263]. Le risque est de « vider de leur substance les règles de protection issues du RGPD en se fondant sur la plasticité de la notion d'intérêt général[1264] ».

Fort heureusement, afin de rétablir la prévalence de protection des données à caractère personnel, le législateur, les autorités administratives indépendantes ou encore la Cour de justice n'hésitent pas à avoir une interprétation extensive des principes. L'extension de la protection des données à caractère personnel au-delà des textes rend la protection quelque peu artificielle, mais considérablement nécessaire.

II. L'extension artificielle de la protection des données à caractère personnel

[1262] Padova Yann, *op. cit*.

[1263] Bergé Jean-Sylvestre et Le Métayer Daniel, « Phénomènes de masse et droit des données », CCE, n° 12, 2018, p. 9 : « Alors que le risque de perte de contrôle sur la circulation des données en général et des masses de données en particulier n'a jamais été aussi grand, une très large partie du discours du droit sur les données demeure rivée sur le contrôle et la possibilité de responsabiliser les acteurs en termes d'anticipation du risque. Tout se passe comme si la situation demeurait durablement sous le contrôle des acteurs et qu'il ne s'agissait pour la règle de droit que de tirer les conséquences ex ante (mise en conformité) ou ex post (responsabilité) des cas de défaut de contrôle. En réalité, comme on l'a déjà vu, l'importance des masses de données en circulation, la rapidité avec laquelle les flux de masses opèrent rendent illusoire toute idée que la situation demeure sous contrôle. Il faut donc prendre la mesure des risques - fussent-ils encore largement invisibles aujourd'hui - qui en découlent. ».

[1264] Favro Karine, « Transformation numérique de l'administration », Dalloz, Répertoire de service public, 2023, point 19 : Libre circulation et mise en cohérence des textes européens.

451. Pouvoirs normatifs. Afin de tempérer la prévalence superficielle de la protection des données à caractère personnel, le législateur n'a pas hésité à user des marges de manœuvre dans le dessein de protéger plus amplement les individus (1). En parallèle, la Cour de justice ainsi que les autorités de régulation et particulièrement la Commission nationale de l'informatique et des libertés, font également usage de leurs pouvoirs d'interprétation afin de renforcer la protection des personnes concernées (2).

A) La normativité protectrice du législateur

452. Cohérence du cadre. L'une des conséquences des négociations engagées pendant l'élaboration du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données est la présence de marges de manœuvre. Le législateur national a fait usage de certaines marges de manœuvre, permettant de protéger davantage les citoyens européens (1). Néanmoins, l'usage des marges de manœuvre a pour conséquence une articulation équivoque entre la loi informatique et libertés et le règlement, impactant la cohérence du cadre normatif (2).

1. L'usage des marges de manœuvre par le législateur

453. Présence des marges de manœuvres dans le RGPD. Malgré l'application directe du règlement dans les ordres juridiques des États membres, le règlement donne une « marge de manœuvre » pour les législateurs nationaux sur certains points identifiés. Lors de la lecture du règlement, plus de cinquante marges de manœuvre sont laissées à l'appréciation des législateurs nationaux[1265]. L'usage intensif des marges de manœuvre dans le règlement sur la protection des données à caractère personnel réduit l'application directe et uniforme, soit les caractères principaux d'un règlement européen. À ce titre, il est possible de parler d'un règlement « hybride », c'est-à-dire mi-règlement, mi-directive, ou encore d'un règlement *sui generis*. En France, le législateur a fait un usage modéré des marges de manœuvre, laissant toutefois

[1265] Conseil d'État, Avis sur un projet de loi portant adaptation au droit de l'Union Européenne de la Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, 7 décembre 2017, p. 3 : Le Conseil d'État a comptabilisé 56 marges de manœuvre au total, prévues soit directement dans les articles du RGPD, soit dans ses considérants.

subsister des interrogations quant à l'articulation entre la loi nationale et le règlement européen. En effet, le législateur a parfois pris des distances avec les marges de manœuvres accordées.

454. Champ d'application territorial renforcé. Tout d'abord, le législateur français a décidé d'exploiter l'une des marges de manœuvre, et non des moindre, concernant le champ d'application territorial du règlement[1266]. En vertu de l'article 3 de Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, les spécificités françaises vont s'appliquer « dès lors que la personne concernée réside en France, y compris lorsque le responsable de traitement n'est pas établi en France ». La notion de « résidence habituelle » est une notion usuelle en droit international privé[1267]. Cependant, la notion retenue dans la Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés est la « résidence » simple, tandis que le Règlement (UE) 2016/679 sur la protection des données à caractère personnel retient la notion de « résidence habituelle »[1268]. Surtout, le législateur déroge à la règle prévue par le règlement selon laquelle la loi applicable est celle du pays dans lequel le responsable de traitement est établi[1269]. Force est de constater que le législateur français a souhaité protéger les résidents français contre les entreprises américaines, dont le siège est en Irlande pour Facebook ou Google, en évitant qu'ils ne se voient appliquer le droit d'un autre État membre. En réalité, le champ d'application de la loi française devient considérablement large, ce qui ne manquera pas de poser des difficultés opérationnelles[1270]. L'objectif du législateur nous semble toutefois louable au regard des pratiques des géants du numérique.

455. Le consentement des mineurs complexifié. Par ailleurs, le législateur français a également usé d'une marge de manœuvre relative au consentement des mineurs. En effet, le règlement sur la protection des données à caractère personnel prévoit une protection particulière. Ce dernier précise que le consentement d'un mineur sur ses données à caractère personnel lorsqu'il recourt à des services numériques ne peut s'effectuer qu'à partir de ses 16

[1266] Griguer Merav, Schwart Julie, « RGPD et loi Informatique et Libertés modifiée. Une harmonie en demi-teinte », Revue Internationale de la Compliance et de l'Éthique des Affaires n° 03, 2018.
[1267] Joubert Natalie, « La dernière pierre (provisoire ?) à l'édifice du droit international privé européen en matière familiale », Revue critique de droit international privé, Dalloz, 2017.
[1268] Au sein de son article 79 relatif au droit à un recours effectif contre le responsable de traitement.
[1269] Bourgeois Matthieu et Moine Marion, « Articulation entre le RGPD et la loi informatique et libertés : le réveil des nations ? », LexisNexis, Cahier législatif nº 280, 2018.
[1270] Debet Anne, « Faut-il réviser la loi informatique et libertés ? », Dalloz IP/IT, 2023, 505 ; Commission nationale de l'informatique et des libertés, délibération, n° 2017-299, p.15 ; Commission nationale de l'informatique et des libertés, délibération n°2018-349, p. 4.

ans[1271]. Sur ce point, le règlement prévoit que les États membres peuvent abaisser cette majorité numérique à 13 ans[1272]. Les géants du numérique ont d'ailleurs tenté d'annuler cette disposition au motif que la variation de seuil de l'âge entre les États membres implique de s'aligner sur le plus exigeant ou d'effectuer des différenciations entre les États membres[1273]. Fort heureusement, et surtout au regard de la nécessaire protection des enfants sur les services numériques, la proposition a été maintenue. Au niveau national, le législateur a fixé la majorité numérique à 15 ans au sein de la loi informatique et libertés, conformément à la faculté laissée par le législateur européen. La délimitation de l'âge était la seule marge de manœuvre dont disposaient les États membres, à l'exclusion de toute autre modification sur le régime applicable pour les mineurs. En réalité, les difficultés vont principalement être d'ordre techniques[1274]. L'effectivité de cette mesure - qu'importe l'âge retenu finalement - pourra être remise en cause en pratique[1275].

2. Les difficultés d'articulation

456. Conflit de « marges ». Lorsque le règlement permet aux États membres de concilier la protection des données à caractère personnel et la liberté d'expression et d'information, le considérant 153 du règlement précise qu'en cas de différences d'exceptions ou de dérogations entre États membres, « le droit de l'État membre dont relève le responsable de traitement

---

1271 Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), article 8 : « Lorsque l'article 6, paragraphe 1, point a), s'applique, en ce qui concerne l'offre directe de services de la société de l'information aux enfants, le traitement des données à caractère personnel relatives à un enfant est licite lorsque l'enfant est âgé d'au moins 16 ans. Lorsque l'enfant est âgé de moins de 16 ans, ce traitement n'est licite que si, et dans la mesure où, le consentement est donné ou autorisé par le titulaire de la responsabilité parentale à l'égard de l'enfant. ».

1272 *Ibid*., article 8.1, alinéa 2 : « Les États membres peuvent prévoir par la loi un âge inférieur pour ces finalités pour autant que cet âge inférieur ne soit pas en-dessous de 13 ans. ».

1273 Rochfeld Judith, « Données à caractère personnel. Données des mineurs », Répertoire IP/IT et Communication, Juillet 2019.

1274 Charrier Benjamin, « Le consentement exprimé par les mineurs en ligne », Dalloz IP/IT, 2018, 333 : « Comment s'assurer que le consentement de l'adulte a effectivement été recueilli ? Une procédure très contraignante ne serait pas réaliste. Il paraît difficilement envisageable de contraindre certains réseaux sociaux, notamment, à recueillir l'envoi par les parents d'un justificatif confirmant à la fois l'autorisation et l'exercice de l'autorité parentale (une copie du livret de famille, par ex.) avant d'ouvrir le compte de chaque mineur de moins de 16 ans (ou 15, 14 ou 13 ans, selon les choix faits par les États membres dans la marge de manœuvre laissée par le RGPD). La question de la mise en œuvre technique des règles nouvelles reste donc entière. ».

1275 *Infra*., n° 509.

devrait s'appliquer[1276] ». En pratique, la formule n'est pas si accessible : s'agit-il du droit de l'État membre où se trouve l'autorité qui contrôle le responsable de traitement ou de renvoyer aux critères nationaux retenus par les États membres, exposant à la « cacophonie[1277] ». Ainsi, les marges de manœuvre risquent d'entraîner des difficultés d'articulation pour la même norme entre les États membres. Surtout, cela va permettre aux acteurs économiques de rechercher le territoire avec la norme la plus avantageuse. *In fine*, les marges de manœuvre entraînent une fragmentation que le règlement voulait précisément éviter. En effet, le dessein du règlement européen sur la protection des données était principalement de rendre uniforme - et donc cohérent - le droit de la protection des données à caractère personnel sur l'ensemble des États membres.

457. Articulation équivoque entre les textes. L'incohérence au niveau national peut d'ores et déjà être soulevée quant au choix symbolique du maintien de la loi informatique et libertés[1278]. Le nombre de renvois opérés dans la loi nationale provoque l'inintelligibilité de certains points du dispositif normatif et le législateur a parfois fait une appréciation déloyale sur certains points à l'égard de l'esprit du texte européen[1279]. Il aurait peut-être été plus judicieux de transposer directement le règlement sur la protection des données à caractère personnel en adaptant les quelques articles soumis aux marges de manœuvre. En pratique, il sera donc question de déterminer quel cadre juridique est à appliquer en priorité : le règlement européen et ne recourir à la Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés qu'en cas de marge de manœuvre ou faut-il appliquer en priorité la loi nationale et ne recourir au

[1276] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)., considérant 153.

[1277] Ancel Marie-Elodie, « À propos de la "marge de manœuvre" laissée par le règlement général sur la protection des données aux États membres de l'Union européenne », Revue critique de droit international prive, n° 3, Dalloz, 2019.

[1278] Desgens-Pasanau Guillaume, « L'articulation des ordres juridiques européen et national à travers l'exemple du règlement général sur la protection des données personnelles », Cahier législatif, 2018.

[1279] Netter Emmanuel, « Le modèle européen de protection des données personnelles à l'heure de la gloire et des périls, », *in* Netter Emmanuel (dir.), *Regards sur le nouveau droit des données personnelles*, éd. Ceprisca, 2019, p. 18 : « Le bilan est donc celui-ci : le droit européen des données à caractère personnel est constitué d'un empilement d'une législation générale et de législations sectorielles, chaque texte étant lui-même d'une grande complexité ; les droits nationaux transposent ensuite les directives et exploitent les "marges de manœuvre" du règlement en ordre dispersé ; la France, pour ce qui la concerne, a produit en retard un texte de son propre aveu inintelligible, et peut être déloyal à l'égard des solutions européennes sur certains points. ».

règlement européen de manière subsidiaire[1280]. En théorie et selon la hiérarchie des normes, le règlement sur la protection des données doit prévaloir sur la loi nationale. La Commission nationale de l'informatique et des libertés a d'ailleurs rappelé qu'il convenait de se référer au règlement et non à la Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés lorsqu'un traitement entre dans le champ d'application du règlement, ce qui est cohérent[1281]. L'usage des marges de manœuvre par le législateur français s'avère donc dans quelques hypothèses contre-productif pour la protection des individus.

Afin d'équilibrer les incohérences du législateur et les intérêts privés des acteurs du numérique, la Cour de justice n'hésite pas à interpréter de manière extensive les principes pour rétablir un équilibre entre pouvoirs et protection des individus.

B) L'interprétation extensive du cadre normatif

458. Extension des notions et pouvoirs. Afin de renforcer la protection des individus, la Cour de justice de l'Union européenne n'hésite pas à retenir une appréciation extensive des notions (1). Par ailleurs, la Loi n° 2024-449 du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique renforce considérablement le pouvoir d'édiction de normes de l'autorité de régulation des données à caractère personnel, s'inspirant directement d'une de ses délibérations. Ainsi, la loi précitée étend également les pouvoirs normatifs de la Commission nationale de l'informatique et des libertés (2).

1. L'appréciation extensive de la protection des individus par la Cour de justice de l'Union européenne

[1280] Martial-Braz Nathalie, Rochfled Judith et Brogli Marine, *Droit des données personnelles*, éd. Dalloz, 2019, p. 20.

[1281] Commission nationale de l'informatique et des libertés, délibération n° 2017-299, 30 novembre 2017 portant avis sur un projet de loi d'adaptation au droit de l'Union européenne de la loi n° 78-17 du 6 janvier 1978, p. 4.

459. Création prétorienne de la Cour de justice de l'Union européenne (CJUE). Pour le droit des données à caractère personnel, la CJUE détient une place cruciale afin de maintenir ou rétablir une certaine cohérence dans l'application et l'interprétation des normes[1282]. Le contrôle par la Cour de justice de l'Union européenne sur l'application des normes renforce la cohérence dans ce système en réseau afin de garantir la sécurité juridique[1283]. Allant encore plus loin dans sa mission d'interprétation, CJUE a déjà devancé le législateur européen en consacrant des droits ne figurant pas littéralement dans les textes, à l'instar du droit au déréférencement[1284]. Il s'agit d'une véritable création prétorienne de la part de la Cour de justice. Pour l'interprétation des normes, la Cour de justice de l'Union européenne dispose d'un rôle renforcé par la possibilité donnée aux hautes juridictions d'interroger la Cour sur l'interprétation du droit de l'Union européenne dans le cadre d'un litige. Ainsi, elle supervise le système en réseau, permettant de rétablir la cohérence entre les États membres. Dans les récentes décisions relatives au règlement sur la protection des données à caractère personnel, la Cour de justice va encore plus loin que les législateurs dans l'interprétation des droits des utilisateurs. Les récentes décisions renforcent le rôle de la Cour et surtout, renforce la protection des utilisateurs contre les usages et pratiques de certains acteurs. Par ces arrêts, la Cour de justice dissuade des responsables de traitement de ne pas respecter le règlement et tente de rééquilibrer les pouvoirs.

460. Élargissement du champ d'application du RGPD. Dans une décision du 20 octobre 2022, la Cour de justice de l'Union européenne a élargi le champ d'application du règlement sur la protection des données[1285]. En effet, la question préjudicielle par la juridiction de renvoi était la suivante : l'article 2, paragraphe 2, sous a), du règlement (UE) 2016/679 devait-il être interprété en ce sens qu'il excluait du champ d'application de ce règlement, le traitement des données à caractère personnel dans le contexte de l'organisation d'élections dans un État

1282 Lafity Elise, « L'articulation des mécanismes de régulation en protection des données personnelles », *in* Bensamoun Alexandra, Bertrand Brunessen et Anca Ailincai Mihaela (dir.), *Le règlement général sur la protection des données : aspects institutionnels et matériels*, éd. Mare & Martin, 2020, p. 244.

1283 Benabou Valérie-Laure « La Cour de justice, gardienne d'une "souveraineté européenne" sur les données », RAE, 2018/1, p. 21 qui évoque « l'ascension de la protection des données à caractère personnel dans la pyramide des normes ».

1284 Quéméner Myriam, « Le Magistrat, régulateur ponctuel, régulateur final », *in* Frison-Roche Marie-Anne (dir.), *Internet, espace d'interrégulation*, éd. Dalloz, 2016, p. 167.

1285 Cour de justice de l'Union européenne, aff. C-306/21, 20 oct. 2022, Komisia za zashtita na lichnite danni, Tsentralna izbiratelna komisia c/ Koalitsia « Demokratichna Bulgaria – Obedinenie ».

membre. Au niveau national, la Commission nationale de l'informatique et des libertés estime que le traitement du Répertoire électoral unique (REU) ne relève pas du champ d'application du règlement[1286]. Dans cette affaire, la Cour de justice estime que les traitements en lien avec les élections, même nationaux, sont soumis au RGPD. Le considérant 16 du règlement exclut uniquement du champ d'application les traitements de données à caractère personnel effectués par les autorités étatiques dans le cadre d'une activité qui vise à préserver la sécurité nationale ou d'une activité pouvant être rangée dans la même catégorie. Selon la Cour, les traitements nationaux en matière électorale, sont compris dans le champ d'application du règlement européen. Ainsi, tous les traitements qui ne sont pas régis par le titre III sur les dispositions applicables aux traitements relevant de la Directive (UE) 2016/680 Police/Justice ou par le Titre IV sur les dispositions applicables aux traitements intéressant la sûreté de l'État et la défense, sont soumis au règlement (UE) 2016/679[1287]. Le champ d'application du règlement devient considérablement large, et cela ne peut qu'être bénéfique pour la protection des individus.

461. Interprétation extensive de l'article 22. Récemment, la Cour de justice s'est également prononcée sur la qualification d'un « score de crédit » comme étant potentiellement une décision automatisée[1288]. Préalablement, un score de crédit est un système d'évaluation permettant de définir la solvabilité d'une personne. Le score de crédit est particulièrement utilisé en matière bancaire pour le remboursement d'un prêt. En pratique, les établissements font appel à des sociétés spécialisées lorsqu'un client souhaite obtenir un prêt bancaire. La difficulté réside dans l'opacité de ces techniques, fondées sur des données à caractère personnel[1289]. L'utilisation de ces pratiques démultiplie les risques pour les personnes évaluées[1290]. En l'espèce, un consommateur s'était vu refuser un prêt par suite d'un mauvais

[1286] Commission nationale de l'informatique et des libertés, délibération n° 2021-008, 14 janvier 2021, portant avis sur un projet de décret modifiant le décret n° 2018-343 du 9 mai 2018 portant création du traitement automatisé de données à caractère personnel permettant la gestion du répertoire électoral unique pris en application des dispositions du I de l'article 2 et de l'article 7 de la loi n° 2016-1048 du 1er août 2016 rénovant les modalités d'inscription sur les listes électorales.

[1287] Debet Anne, « La CJUE étend, une nouvelle fois, le champ d'application du RGPD », CCE, n° 1, janvier 2023, 5.

[1288] Cour de justice de l'Union européenne, aff. C-634/21, 7 déc. 2023, Schufa Holding AG.

[1289] Jean-Marc Deltorn, « Le droit des données personnelles face à l'opacité des algorithmes prédictifs : les limites du principe de transparence », *in* Netter Emmanuel (dir.), *Regards sur le nouveau droit des données personnelles*, éd. Ceprisca, 2019, p. 153.

[1290] Merabet Samir « Droit et Intelligence artificielle - Chronique », La Semaine Juridique, édition générale n° 25, juin 2024, doctr. 820, v° 5 - Protection des personnes contre les décisions entièrement automatisées et scoring bancaire.

score, il souhaitait par conséquent exercer son droit d'accès et d'effacement. La question préjudicielle posée à la Cour de justice était de savoir si le score de crédit constituait une décision fondée exclusivement sur un traitement automatisé, entraînant l'application de l'article 22 du RGPD. La Cour de justice répond par l'affirmative, un score de crédit constitue effectivement une décision exclusivement fondée sur un traitement automatisé ayant des effets significatifs lorsque la décision prise par une tierce partie est déterminée significativement par ce score[1291].

Ainsi, la Cour de justice retient une interprétation large des trois critères de l'article 22[1292]. L'interprétation extensive par la Cour de justice de l'article 22 est louable et aura des conséquences indéniables en pratique. En effet, cela implique que le régime d'interdiction de l'article s'appliquera pour des cas similaires comme l'algorithme de Parcoursup, le classement des informations sur les réseaux sociaux ou encore les algorithmes de détection de fraude par la CAF[1293]. À l'heure de l'essor des applications de l'intelligence artificielle, cette solution était indispensable pour la protection des individus. En réalité, la CJUE retient une interprétation extensive certes, toutefois conforme à l'ambition du texte selon laquelle le destin des individus ne doit pas être régi exclusivement par un algorithme[1294]. À cet égard, la Cour de justice rappelle qu'une interprétation restrictive aurait renforcé le risque de contournement de cet article et par la suite, une lacune dans la protection juridique[1295].

1291 Cour de justice de l'Union européenne, aff. C-634/21, 7 déc. 2023, Schufa Holding AG, point 73 : « l'établissement automatisé, par une société fournissant des informations commerciales, d'une valeur de probabilité fondée sur des données à caractère personnel relatives à une personne et concernant la capacité de celle-ci à honorer des engagements de paiement à l'avenir constitue une "décision individuelle automatisée" », dès lors que « dépend de manière déterminante de cette valeur » le fait « qu'une tierce partie, à laquelle ladite valeur de probabilité est communiquée, établisse, exécute ou mette fin à une relation contractuelle avec cette personne ».

1292 Douville Thibault, « De l'approche extensive de la prise de décision exclusivement automatisée », D., 2024, 1000.

1293 Huttner Liane, « Décisions automatisées : le réveil d'un géant endormi ? », CCE, n° 2, février 2024, étude 3.

1294 Netter Emmanuel, « Quand la force de conviction du scoring bancaire provoque sa chute. L'interprétation extensive, par la CJUE, de la prohibition des décisions entièrement automatisées », RTD com, 2024, 342.

1295 Cour de justice de l'Union européenne, aff. C-634/21, 7 déc. 2023, Schufa Holding AG, point 61 : « il existerait un risque de contournement de l'article 22 du RGPD et, par suite, une lacune dans la protection juridique si une interprétation restrictive de cette disposition était retenue, selon laquelle l'établissement de la valeur de probabilité doit seulement être considéré comme un acte préparatoire et seul l'acte adopté par la tierce partie peut, le cas échéant, être qualifié de "décision", au sens de l'article 22, paragraphe 1, de ce règlement. »

Par ailleurs, la Commission nationale de l'informatique et des libertés n'hésite pas à renforcer ses pouvoirs normatifs.

2. L'extension des pouvoirs normatifs des autorités par la SREN

462. Délibération de la formation restreinte de la CNIL[1296]. Le 20 décembre 2022, à l'issue d'une procédure de sanction à l'égard de la société américaine LUSHA, la Commission nationale de l'informatique et des libertés n'a pas eu le choix de décider que le RGPD n'était pas applicable, prononçant un non-lieu. En l'espèce, la société américaine fournissait une extension pour navigateur qui révèle à ses clients les coordonnées professionnelles (numéro de téléphone et adresse électronique) de personnes cibles depuis certains réseaux sociaux professionnels et plateformes de relations clients. L'extension fonctionnait grâce à des applications mobiles développées par des filiales israéliennes. En application du règlement sur les données à caractère personnel, la Commission nationale de l'informatique et des libertés a estimé que le règlement ne pouvait s'appliquer. En effet, la société ne disposait pas d'établissement dans l'Union européenne, puisque la société était basée aux États-Unis et ses filiales en Israël, de sorte que le critère de l'établissement n'était pas caractérisé ; l'extension n'était pas liée à une offre de biens ou de services au motif que la société offrait ses services aux utilisateurs de l'extension et non aux personnes dont les données étaient collectées et pour finir, les personnes concernées ne faisaient pas l'objet d'un suivi de comportement au sein de l'Union européenne.

Selon la formation restreinte « la constitution de la base de données par la société repose uniquement sur le rapprochement entre des données de contacts professionnels (téléphone, adresse électronique) avec l'identité des personnes dont le profil est visité sur LinkedIn afin d'en vérifier la véracité. Il ne s'agit donc pas, en l'espèce, d'un traitement qui consiste à analyser ou prédire un comportement, les préférences personnelles ou les déplacements d'une personne, ses intérêts, sa situation économique ou son état de santé[1297]. ». Ainsi, en l'absence d'établissement dans l'Union européenne et en l'absence d'un suivi de comportement, le règlement sur la protection des données à caractère personnel (RGPD) n'était pas applicable à ladite société. Afin d'étendre l'applicabilité du règlement sur la protection des données à

[1296] Commission nationale de l'informatique et des libertés, Délibération de la formation restreinte n° SAN-2022-024 du 20 décembre 2022 concernant la société LUSHA SYSTEMS INC.
[1297] *Ibid*., point 47.

caractère personnel, la SREN donne compétence à la Commission nationale de l'informatique et des libertés pour les prochains litiges à ce sujet.

463. Article 60 SREN. Dans le dessein d'étendre la compétence matérielle de la Commission nationale de l'informatique et des libertés dans la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, l'article 60 de la SREN prévoit que « Les titres Ier et II de la présente loi s'appliquent notamment aux traitements de données à caractère personnel de personnes qui se trouvent sur le territoire français par un responsable du traitement ou un sous-traitant qui n'est pas établi dans l'Union européenne lorsque ces traitements sont liés au suivi du comportement de ces personnes au sein de l'Union européenne, notamment par la collecte de leurs données à caractère personnel en vue de leur rapprochement avec des données liées à leur activité en ligne. ». Désormais, la pratique de rapprochement de données - même issues de différents ensembles de données - pourra être considérée comme un traitement de « suivi » des personnes[1298]. L'extension des pouvoirs de la Commission nationale de l'informatique et des libertés semble justifiée au regard des pratiques des géants du numérique. La Commission nationale de l'informatique et des libertés doit être dotée de pouvoirs renforcés afin de pouvoir faire face aux acteurs du numérique. La Commission nationale de l'informatique et des libertés ne doit pas simplement exister pour élaborer des normes, elle doit avoir la capacité de sanctionner les pratiques néfastes : il est nécessaire d'adapter les pouvoirs aux usages.

464. Conclusion de la section. L'ensemble du droit des données s'est construit autour du règlement sur la protection des données à caractère personnel. La protection des données à caractère personnel pour les utilisateurs est devenue un droit fondamental, protégé par la Charte

[1298] Schwartz Julie et Schlich Rémy, « Loi SREN : de nouveaux pouvoirs pour la CNIL », Cahiers de droit de l'entreprise n° 3, Mai-Juin 2024.

des droits fondamentaux. Désormais, l'ensemble des règlements sur les données doivent respecter la norme suprême de protection des données à caractère personnel. De ce fait, l'ensemble des règlements considèrent l'éventuel conflit de lois entre les différents objectifs d'ouverture et de protection. Sans exception, les divers règlements doivent s'appliquer sans préjudice du RGPD, conférant une prévalence incontestable du règlement en théorie.

En pratique, la protection fondamentale des données à caractère personnel s'avère superficielle. La multiplicité des règlements entraîne le chevauchement de certaines notions et l'articulation devient complexe. La complexité des divers régimes applicables est à nouveau favorable aux acteurs du numérique. Ils avancent sans cesse de nouvelles interprétations textuelles afin d'appliquer la règle la plus favorable pour faire perdurer leurs pratiques. Par ailleurs, le développement des technologies émergentes et particulièrement l'intelligence artificielle bouleversent la prévalence théorique des données à caractère personnel. La prévalence devient contestable au regard des flux de données utilisés pour le développement de l'intelligence artificielle. De surcroît, les récents règlements accentuent l'ouverture des données afin de privilégier les usages d'intelligence artificielle. *In fine*, les pratiques de *lobbying* et de privation des normes ont finalement permis aux acteurs du numérique de rendre la prévalence des données à caractère personnel superficielle.

Afin de restituer la prévalence des données à caractère personnel, le législateur national a fait un usage des marges de manœuvre pour étendre la protection des individus sur le territoire. En parallèle, la Cour de justice ainsi que les autorités administratives indépendantes profitent de leur pouvoir d'interprétation afin de renforcer la protection des individus. La Cour de justice n'hésite pas à interpréter les notions du RGPD de manière extrêmement large afin de contrer la puissance des acteurs du numérique et de confirmer sa place prééminente pour tenter de rétablir la cohérence du cadre normatif. La Commission nationale de l'informatique et des libertés quant à elle n'hésite pas également à solliciter l'adaptation de ses pouvoirs aux nouveaux usages. Il est louable que les autorités légitimes renforcent enfin leurs pouvoirs et affirment leurs compétences afin de rétablir un équilibre entre les puissances.

465. Conclusion du chapitre. L'usage intensif des données par les acteurs du numérique a bouleversé la pyramide des normes. Le législateur partage son pouvoir avec des autorités administratives indépendantes et des acteurs privés. Les autorités et les acteurs privés ont pour

similitude de constituer un relais pour le législateur dans un domaine technique. Le pouvoir normatif est partagé pour développer des normes flexibles afin de ne pas brider l'innovation.

En effet, la régulation complète la réglementation, étant regardée comme inflexible et obsolète dans le domaine des données. En revanche, la régulation permettrait de s'adapter à chaque secteur et de développer des normes de droit souple. Toujours dans le dessein de s'adapter à cet environnement sans frontière et mouvant, un système de *compliance* s'est développé au profit des acteurs du numérique. Ils deviennent les plus à même de développer leurs propres normes pour s'adapter à leurs techniques.

En réalité, la privatisation de l'élaboration des normes est favorable aux acteurs du numérique. La logique de prévention et d'accompagnement leur permet de développer des technologies toujours plus intrusives pour la vie privée des individus. Pour eux, la priorité de la protection des données à caractère personnel est une prévalence principalement théorique. Ils contournent sans cesse le régime de protection des données à caractère personnel afin de développer des technologies lucratives. Par ailleurs, l'internalisation des normes leur permet de rendre encore plus complexe l'articulation des normes. En effet, ils sont les protagonistes de cette complexité et ont tout intérêt à faire perdurer l'incohérence du cadre : la multiplicité des normes et des acteurs de la régulation profite à ces acteurs privés. Le modèle en réseau des normes propose une alternative radicale et décentralisée au modèle pyramidal, remettant en cause les hiérarchies établies offrant une vision subversive de la régulation.

Il est nécessaire de rétablir un équilibre entre les pouvoirs en excluant leur présence dans la construction du cadre normatif et en redonnant les pouvoirs aux acteurs légitimes. De surcroît, l'important est désormais de privilégier les directives du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 et son interprétation extensive par les instances, qu'il s'agisse de la Cour de justice de l'Union européenne ou des autorités administratives indépendantes. La prévalence du RGPD ne doit plus être superficielle mais bien réelle dans les pratiques du numérique.

466. Conclusion du Titre. L'environnement numérique et particulièrement les flux des données ont bouleversé la pyramide des normes. Le droit des données est un droit complexe évoluant dans un environnement contrôlé par de puissants acteurs privés. La logique

pyramidale, dominée par le monopole d'édiction des normes par l'État est devenue archaïque. En effet, la logique kelsienne a été substituée par une logique de gouvernance. La gouvernance est un changement de paradigme dominé par la croyance dans l'autorégulation des groupes sociaux et le recul de l'État. Les groupes sociaux, c'est-à-dire les entreprises privées, sont les protagonistes de la technicité de leur propre environnement et seraient donc les plus idoines à élaborer des normes.

Le législateur partage également son pouvoir avec les autorités administratives indépendantes censées réguler les secteurs techniques. Les flux de données ont transcendé une grande partie des secteurs régulés. De ce fait, les autorités administratives indépendantes se sont multipliées et diversifiées. La logique de la régulation est dominée par l'incitation et non plus la contrainte, afin de s'adapter à cet environnement technique. Les acteurs deviennent responsables de leurs développements technologiques et techniques. Leurs pratiques étant majoritairement opaques, la logique de responsabilité devient internalisée.

En réalité, les acteurs du numérique ne sont pas légitimes à participer à la construction du cadre normatif. La privatisation des normes est un danger pour la cohérence des normes : ils participent à l'élaboration des normes, s'érigent en régulateur privé et utilisent le code comme source de droit. Grâce à l'autorégulation et l'élaboration des normes de droit souple, ils s'imbriquent dans chaque étape de la construction. En amont par leurs pratiques de *lobbying* et par la suite au sein de leur processus avec l'autorégulation. La privatisation des normes leur permet d'exercer un *lobbying* extrêmement précis et d'identifier les normes à éviter. En effet, ils élaborent leurs propres règles en ayant la parfaite maîtrise de leurs pratiques et de leur environnement. L'ensemble de leurs pratiques est opaque et constitue un réel danger pour l'exercice des droits des individus.

La participation de ces acteurs privés pour la construction du cadre normatif ne doit pas perdurer au nom de l'innovation. Il est nécessaire de rétablir un équilibre entre les pouvoirs en excluant leur présence et en redonnant les pouvoirs aux acteurs légitimes. Pour ce faire, les autorités administratives indépendantes sont légitimes et nécessaires afin de garantir le respect de la vie privée et la protection des données à caractère personnel des utilisateurs. *In fine*, les juges et les autorités administratives indépendantes sont les garants de la cohérence d'un système en réseau.

Finalement, la cohérence du cadre normatif réside dans le respect du droit à la protection des données à caractère personnel des individus. Dès lors que cette prévalence n'est pas respectée, le cadre normatif ne peut pas être effectif.

TITRE 2 : L'EFFECTIVITÉ LIMITÉE DU CADRE NORMATIF

> *« Si la règle inappliquée n'en reste pas moins la règle, on saisit l'enjeu que représente l'application, dans un climat social et juridique qui manifeste tout à la fois - ce qui n'est d'ailleurs pas contradictoire - un besoin de meilleure adéquation et de plus grande libéralisation, surtout dans certains domaines particulièrement imprégnés de droit. L'inapplication de la règle peut d'ailleurs être insupportable dès lors qu'elle est respectée par certains et ignorée par d'autres, sans qu'aucune conséquence n'en découle pour ces derniers. L'ineffectivité signe alors une rupture d'égalité devant le droit*[1299]*. »*

467. Prévalence des données à caractère personnel. Afin d'être effectif, le cadre normatif doit respecter dans un premier temps le droit des données à caractère personnel. Au regard de la prévalence de ce droit dans le réseau de normes, les règles doivent être appliquées effectivement pour garantir la cohérence du cadre normatif. En effet, les normes concernant la protection des données à caractère personnel ont été promulguées depuis plus de quatre décennies. Néanmoins, la mise en œuvre du cadre normatif a fait l'objet d'une application lacunaire pendant longtemps : il s'agissait davantage d'un système préventif plutôt qu'un réel système répressif. L'insuffisante mise en œuvre du droit des données a permis de faire prospérer des traitements illicites de données.

468. Notion d'effectivité. Pour le moment, il existe une divergence notable entre la lecture des textes et la réalité des traitements. Pourtant, c'est la mise en œuvre effective du cadre normatif qui permet d'assurer la protection des individus. L'effectivité peut être définie comme

[1299] Terré François et Molfessis Nicolas, *Introduction générale au droit*, éd. Dalloz, 2022, p. 824.

le degré de réalisation, dans les pratiques sociales, des règles énoncées par le droit[1300] : il s'agit alors de mesurer les écarts entre le droit en vigueur et la réalité sociale. L'effectivité d'un cadre normatif s'apprécie dans la réalité des faits. Au niveau de l'Union européenne, la notion d'effectivité est cardinale puisqu'elle constitue un fondement et dispose d'une valeur constitutionnelle en droit européen[1301]. Le droit de l'Union européenne s'est construit autour de cette notion et fonde une partie de sa légitimité. Selon une approche sociétale, l'effectivité aurait pour objet de « mettre en lumière les effets du droit de l'Union européenne sur la société, sa capacité à modeler les situations sociales, à être la traduction d'un certain modèle social[1302] ». *In fine,* l'effectivité serait une condition « globale » de la validité d'un système de normes[1303].

469. Annonce de plan. Afin d'étudier l'effectivité du cadre normatif, il convient dans un premier temps d'analyser l'effectivité au regard de mise en œuvre des normes, c'est-à-dire la réception des règles par ses destinataires (**Chapitre 1**). De surcroît, l'étude de l'effectivité des sanctions doit compléter l'effectivité des normes : la réelle mise en œuvre des sanctions est une condition nécessaire à l'effectivité du cadre normatif. Le rôle dissuasif et la mise en œuvre du cadre répressif permettent d'analyser l'effectivité au regard de l'application des sanctions (**Chapitre 2**).

1300 Arnaud André Jean, *Dictionnaire encyclopédique de théorie et de sociologie du droit*, 2018, p. 217.

1301 Deffains Bruno, « Approche économique de l'effectivité du droit européen », *in* Bouveresse Aude, Ritleng Dominique (dir.), *L'effectivité du droit de l'Union européenne*, éd. Bruylant, 2018, p. 33 ; Traité sur le Fonctionnement de l'Union européenne, article 19 qui dispose que « les États membres établissent les voies de recours nécessaires pour assurer une protection juridictionnelle effective dans les domaines couverts par le droit de l'Union » ; Charte des droits fondamentaux de l'Union européenne qui dispose également que : « toute personne dont les droits et libertés garantis par le droit de l'Union ont été violés à droit à un recours effectif devant un tribunal dans le respect des conditions prévues au présent article ».

1302 Bouveresse Aude et Ritleng Dominique, « Avant-Propos », *in* Bouveresse Aude, Ritleng Dominique (dir.), *L'effectivité du droit de l'Union européenne*, éd. Bruylant, 2018, p. 6.

1303 Dubout Édouard, « Être ou ne pas être (du droit) ? Effectivité et champ d'application du droit de l'Union européenne », *in* Bouveresse Aude, Ritleng Dominique (dir.), *L'effectivité du droit de l'Union européenne*, éd. Bruylant, 2018, p. 87.

Chapitre 1 :

Les limites de l'effectivité des règles

470. Effets sur les comportements. Le cadre normatif sert à orienter les comportements de ses destinataires dans un sens voulu par le législateur[1304] : l'effectivité est appréciée en fonction des effets réels sur les comportements sociaux et lorsque la norme produit l'effet voulu sur les personnes concernées, la règle peut être qualifiée d'effective[1305]. En réalité, Jean Carbonnier estimait qu'entre « l'effectivité totale et l'ineffectivité totale, également exceptionnelle, c'est la grisaille de l'ineffectivité partielle qui domine[1306] ». Ainsi, l'effectivité doit être appréciée en termes de degrés et selon les effets produits sur les comportements sociaux, qu'il s'agisse des individus ou des protagonistes.

Afin de protéger les individus contre les traitements illicites, le cadre normatif a instauré des principes protecteurs pour les personnes concernées et des obligations pour les acteurs impliqués. À cette fin, le principe du consentement a été promulgué pour les individus comme une réelle possibilité de reprendre le contrôle et la maîtrise de l'usage de leurs données et par conséquent, de garantir l'effectivité de leur protection. Par ailleurs, d'autres principes ont été imposés aux responsables de traitements - tels que le principe de minimisation, de finalité ou encore d'effacement - afin de limiter les traitements abusifs de données.

471. Réalité des traitements. Les principes protecteurs peuvent être qualifiés d'effectifs dès lors que les intéressés s'y soumettent et que ces derniers produisent de réels effets sur les comportements. Or, les géants du numérique ne cessent de développer de nouvelles techniques de manipulation afin de spécifiquement contourner les principes protecteurs. De fait, ils peuvent perpétuer certains traitements illicites déjà exploités pendant de nombreuses années. Le développement des technologies émergentes permet également de contourner le cadre normatif pour les acteurs du numérique.

[1304] Ost Francois et Van de Kerchove Michel, *De la pyramide au réseau. Pour une théorie dialectique du droit,* éd. FUSL, 2022, p. 329.
[1305] Bergel Jean-Louis, *Théorie générale du droit*, éd. Dalloz, 2012, p. 168.
[1306] Jean Carbonnier, « Les phénomènes d'incidence dans l'application des lois », *Flexible droit. Pour une sociologie du droit sans rigueur*, éd. LGDJ, 2001, p. 146.

472. Annonce de plan. Ainsi, l'effectivité des principes peut être remise en cause en raison de leur idéalisme au regard de la réalité sociale. En effet, cette effectivité va être tant confrontée aux pratiques des géants du numérique (**Section 1**) qu'au rythme des technologies émergentes (**Section 2**).

Section 1 : Le principe limité du consentement face aux pratiques des géants du numérique

473. Pouvoir des individus. Le dessein du droit des données à caractère personnel est d'accroître l'effectivité de la protection des individus. Pour ce faire, il convient de renforcer la possibilité pour les individus de contrôler leurs données : les individus doivent pouvoir décider du traitement de leurs données à caractère personnel. Il s'agit de redonner le pouvoir aux individus de consentir ou non à un traitement sur leurs données à caractère personnel.

474. Annonce de plan. En théorie, le choix de consentir à un traitement a été renforcé par le règlement sur la protection des données à caractère personnel (I). En pratique, les géants du numérique développent sans cesse des technologies afin de limiter cette liberté de choix (II).

I. Le renforcement du principe en théorie

475. Analyse de la notion. Afin de déterminer la place du consentement, il convient dans un premier temps de revenir sur la notion du consentement en droit de la protection des données à caractère personnel (A). L'analyse de cette notion permettant d'analyser la valeur surestimée du consentement dans l'univers numérique (B).

A) La notion spécifique du consentement

476. Définition du consentement. La notion de consentement fait l'objet d'une définition propre dans le Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (1). Afin d'être valable, le consentement doit revêtir plusieurs caractères (2).

1. La définition précise du consentement

477. Rôle symbolique du consentement. Tout d'abord, le consentement possède un rôle symbolique en matière de protection des données à caractère personnel. En effet, la Charte des droits fondamentaux de l'Union européenne dispose que les données doivent être traitées « sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi[1307] ». Dès lors, le consentement apparaît comme une base juridique prioritaire pour les traitements de données à caractère personnel[1308] : chaque individu aurait le choix de consentir ou non à un traitement sur ses données à caractère personnel. Le consentement permettrait alors aux personnes concernées de contrôler pleinement l'usage de leurs données[1309], devenant une composante du droit à l'autodétermination informationnelle[1310].

478. « Empowerment » des individus. L'expression du consentement illustrerait un certain « empowerment » de l'individu sur ses données[1311], c'est-à-dire une capacité d'agir pour son bien-être[1312]. La notion d'*empowerment* repose sur deux composantes principales : la capacité pour l'individu de décider d'agir dans son intérêt ainsi que l'opportunité d'exercer effectivement ses propres décisions. Il existe plusieurs dimensions de l'*empowerment* dont « l'agentivité » des individus - notion issue des sciences sociales -, pouvant être transposée en matière de protection des données à caractère personnel[1313]. L'agentivité suppose que l'individu puisse être en mesure d'exprimer son consentement sous réserve d'avoir accès à l'information

---

[1307] Charte des droits fondamentaux de l'Union européenne, article 8.2 : « Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification. ».

[1308] Vergnolle Suzanne, *L'effectivité de la protection des personnes par le droit des données à caractère personnel*, éd. Larcier, 2022, p. 273.

[1309] Groupe de travail sur l'article 29 (G29), « Lignes directrices sur le consentement au sens du règlement 2016/279 », WP259, 10 avril 2018.

[1310] Rouvroy Antoinette et Poullet Yves, « Le droit à l'autodétermination informationnelle et la valeur du développement personnel », État de droit et virtualité, 2009, pp. 157-222 ; Poullet Yves « Consent : "The privacy bug" », *in* Giudicelli André et Caprioli Éric, *La confiance numérique*, éd. LexisNexis, 2022, pp. 75-117 : « Le consentement apparaît par ailleurs comme la consécration la plus évidente du droit à l'"autodétermination informationnelle", qui fonde le régime de protection des données et s'entend comme la liberté de principe de consentir au traitement des données à caractère personnel. ».

[1311] Debet Anne, « Le consentement dans le Règlement Général sur la Protection des données : rôle et définition », CCE, n° spécial avril 2018, étude n° 9.

[1312] Calvès Anne-Emmanuèle, « Empowerment », Revue Tiers Monde, 200, Armand Colin, 2009.

[1313] Anciaux Nicolas et Zolynski Célia, « Empowerment et Big Data sur données personnelles. De la portabilité à l'agentivité », *in* Florence G'Sell (dir.), *Le Big Data et le Droit*, éd. Dalloz, 2020, p. 220.

nécessaire et surtout, que l'individu soit en mesure de comprendre ladite information. Au sein de cette conception symbolique, le consentement serait un outil idéal et infaillible permettant aux individus de maintenir le contrôle sur leurs propres données.

479. Définition du consentement. Par-delà la conception symbolique, la notion de consentement est une notion cardinale en droit des contrats. Il s'agit d'un « accord de volontés entre deux ou plusieurs personnes destiné à créer, modifier, transmettre ou éteindre des obligations[1314] ». Au sens étymologique, le terme consentement désigne l'accord de deux volontés, c'est à dire celle du débiteur qui s'oblige et celle du créancier envers lequel il s'oblige[1315] : le consentement est une rencontre de volontés[1316]. Dans une approche classique et libérale, cette rencontre de volontés résulte de personnes en situation d'égalité, qui ont librement et rationnellement consenti à s'obliger, afin de concrétiser un échange économique servant des intérêts réciproques[1317]. La situation d'égalité entre les contractants a rapidement été remise en cause au regard des inégalités de fait[1318]. En effet, il existe des déséquilibres de force entre les parties, résultant d'une partie « forte » et d'une partie « faible ». En matière de protection des données à caractère personnel, il existe effectivement un déséquilibre entre les parties puisque les acteurs du numérique détiennent un pouvoir certain sur les individus.

480. Définition spécifique. Afin de tempérer le déséquilibre entre les parties, le droit de la protection des données à caractère personnel a renforcé la notion du consentement par la définition qui suit : « toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement[1319] ». Le consentement serait alors l'expression parfaite de l'autonomie de la volonté, la volonté de

---

1314 Code civil, article 1101.

1315 Terré François, Simler Philippe et Lequette Yves, *Droit civil. Les obligations*, éd. Dalloz, 2018, p. 183.

1316 Cornu Gérard, *Vocabulaire juridique*, éd. PUF, 2020, v° « Consentement », sens 1, p. 241.

1317 Rochfeld Judith, *Les grandes notions du droit privé*, éd. PUF, 2022, p. 530.

1318 *Ibid.*, p. 541 : « Pour en arriver là, il a fallu relever, dès la fin du XIXème siècle, un accroissement des inégalités économiques des parties. Celles-ci existeraient déjà du temps du Code civil. Mais la proclamation de l'égalité abstraite et juridique des citoyens, ainsi que le maintien de ces inégalités à des échelles individuelles, avaient fait obstacle à la reconnaissance de ces déséquilibres. Ce constat ne pourra cependant plus être éludé face au développement des relations de travail inégalitaires, où le salarié ne peut guère négocier et imposer ses conditions contractuelles à un employeur ; à la généralisation des rapports impersonnels et standardisés entre consommateurs et professionnels. ».

1319 Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, article 4.11.

l'individu étant la source essentielle de ses obligations[1320]. De par cette conception individualiste, un individu ne pourrait se trouver dans les liens d'un contrat sans l'avoir voulu[1321]. En matière de protection des données à caractère personnel, il appartiendra au responsable de traitement de démontrer que la personne a consenti au traitement de ses données à caractère personnel en vertu du principe d'*accountability*. En outre, il devra démontrer que la manifestation de volonté a été libre, spécifique, éclairée et univoque afin d'être valable.

2. Les caractères du consentement valable

481. Un consentement libre. Le caractère libre du consentement se caractérise par un véritable choix de l'utilisateur sur ses données. En ce sens, le consentement est libre lorsque la personne concernée « dispose d'un contrôle et d'un choix réel concernant l'acceptation ou le refus des conditions proposées ou encore de la possibilité de les refuser sans subir de préjudice[1322] ». Le choix réel de consentir découlerait d'une certaine « capabilité » des individus, c'est-à-dire la capacité des individus de faire des choix libres[1323]. La personne concernée doit pouvoir exercer son choix de manière libre sans subir de conséquence négative. À titre d'illustration, la Commission nationale de l'informatique et des libertés considère que le consentement de l'utilisateur d'un réseau social n'est pas donné librement lorsque le refus de consentement implique la suppression du compte[1324]. Dès lors, lorsque l'utilisateur refuse un

1320 Terré François, Simler Philippe, Lequette Yves, *op. cit*., p. 32.

1321 Carbonnier Jean, *Droit civil. Les biens,* éd. PUF, 2004, p. 1976.

1322 Groupe de travail sur l'article 29 (G29), « Lignes directrices sur le consentement au sens du règlement 2016/679 », adoptées le 28 novembre 2017, version révisée et adoptée le 10 avril 2018, p. 3 : « En général, le consentement ne constitue une base juridique appropriée que si la personne concernée dispose d'un contrôle et d'un choix réel concernant l'acceptation ou le refus des conditions proposées ou de la possibilité de les refuser sans subir de préjudice. Lorsqu'il sollicite un consentement, le responsable du traitement a l'obligation d'évaluer si celui-ci satisfera à toutes les conditions d'obtention d'un consentement valable. S'il a été obtenu dans le plein respect du RGPD, le consentement est un outil qui confère aux personnes concernées un contrôle sur le traitement éventuel de leurs données à caractère personnel. Dans le cas contraire, le contrôle de la personne concernée devient illusoire et le consentement ne constituera pas une base valable pour le traitement des données, rendant de ce fait l'activité de traitement illicite. ».

1323 La théorie des « capabilité » est issue de l'économiste Amartya Sen (prix nobel d'économie en 1998). Il estime que « les inégalités entre les individus ne s'apprécient pas au regard de leurs seules dotations en ressources mais de leurs capacités à les convertir en libertés réelles », disponible sur économie.gouv.

1324 Commission nationale de l'informatique et des libertés, décision n° SAN-2017-075, 27 novembre 2017 : Le litige concernait la transmission de données de WhatsApp à Facebook. En effet, le seul moyen de s'opposer à la transmission des données pour la finalité accessoire de « business intelligence » était de désinstaller l'application. Ainsi, le consentement n'était pas donné librement par les utilisateurs ; Vincent Téchené, « Transmission de données de Whatsapp à Facebook : mise en demeure publique pour absence de base légale », Le Quotidien, janvier 2018.

traitement sur ses données à caractère personnel, une alternative doit lui être proposée afin de bénéficier d'un service équivalent. Lorsque la personne concernée ne dispose pas d'un choix alternatif, le consentement est considéré comme illusoire.

482. Absence de déséquilibre. Par ailleurs, le caractère libre du consentement implique l'absence de déséquilibre entre le responsable de traitement et la personne concernée. Le déséquilibre peut être caractérisé dans le cadre des relations entre employeur et employés ou encore des relations entre administration et usager[1325]. La Commission nationale de l'informatique et des libertés rappelle à ce titre que les employés sont très rarement en mesure de donner un consentement libre au regard de la dépendance qui découle de la relation avec l'employeur[1326]. Il peut également exister un déséquilibre entre les professionnels et les consommateurs. Le consentement sera présumé illicite lorsqu'il existe une altération de la liberté de choix de l'individu du fait d'un déséquilibre entre les individus[1327].

483. Retrait du consentement. Enfin, le caractère libre du consentement s'illustre également avec la possibilité de retirer son consentement[1328]. L'utilisateur doit pouvoir retirer son consentement à tout moment : les modalités de retrait doivent être équivalentes à celle utilisée pour recueillir le consentement. Le groupe de travail G29 exige un « parallélisme des formes » concernant le recueil du consentement et le retrait de ce dernier[1329]. Par exemple, lorsque les modalités ont été faites en ligne, le retrait doit également pouvoir se faire en ligne. Lorsque l'individu exerce son droit de retrait, les traitements effectués avant le retrait demeurent

---

1325 Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, considérant 43 : « Pour garantir que le consentement est donné librement, il convient que celui-ci ne constitue pas un fondement juridique valable pour le traitement de données à caractère personnel dans un cas particulier lorsqu'il existe un déséquilibre manifeste entre la personne concernée et le responsable du traitement, en particulier lorsque le responsable du traitement est une autorité publique et qu'il est improbable que le consentement ait été donné librement au vu de toutes les circonstances de cette situation particulière. ».

1326 Commission nationale de l'informatique et des libertés, délibération n° SAN-2019-160, 21 novembre 2019 portant adoption du référentiel relatif aux traitements de données personnelles mis en œuvre aux fins de gestion des ressources humaines.

1327 Martial-Braz Nathalie, Rochfled Judith et Brogli Marine, *Droit des données personnelles. Les spécificités du droit français au regard du RGPD*, éd. Dalloz, 2019, p. 154.

1328 Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, article 7, point 3 : « La personne concernée a le droit de retirer son consentement à tout moment. Le retrait du consentement ne compromet pas la licéité du traitement fondé sur le consentement effectué avant ce retrait. La personne concernée en est informée avant de donner son consentement. Il est aussi simple de retirer que de donner son consentement. ».

1329 Groupe de travail sur l'article 29 (G29), *op. cit*., p. 25.

légitimes. Le retrait n'a d'effet que pour les traitements futurs. L'affirmation du principe de droit au retrait constitue *a priori* un renforcement du consentement des personnes concernées[1330].

484. Un consentement spécifique. D'autre part, le consentement doit être spécifique, c'est-à-dire correspondre à un seul traitement pour une finalité déterminée[1331] : lorsque le traitement comporte plusieurs finalités, un consentement distinct doit être recueilli pour chaque finalité. Afin de se conformer au caractère spécifique du consentement, le responsable de traitement doit garantir la spécification des finalités en tant que garantie contre tout détournement d'usage, le caractère détaillé des demandes de consentement et la séparation claire des informations liées à l'obtention du consentement au traitement des données[1332]. La séparation claire des informations permet d'interdire les demandes de consentement « en bloc ». En effet, lorsque la personne concernée accepte un ensemble de traitement par bloc, le consentement ne sera pas spécifique[1333] puisqu'un consentement global pour différentes finalités n'est pas valable[1334]. Le caractère spécifique permet à l'utilisateur de garder le contrôle sur ses données et est donc intrinsèquement lié à la notion de liberté de choix de l'utilisateur.

485. Un consentement univoque. S'agissant du recueil du consentement, le considérant 32 du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données précise que « le consentement devrait être donné par un acte positif clair par lequel la personne concernée manifeste de façon libre, spécifique, éclairée et univoque son accord au traitement des données à caractère personnel la concernant, par

---

1330 Boizard Maryline, « Le consentement à l'exploitation des données à caractère personnel : une douce illusion ? », CCE, n°3, étude 6, 2016.

1331 Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, article 6.1 : « 1. Le traitement n'est licite que si, et dans la mesure où au moins une des conditions suivantes est remplie : a) La personne concernée a consenti au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques. ».

1332 Groupe de travail sur l'article 29 (G29), *op. cit*., p. 16.

1333 Commission nationale de l'informatique et des libertés, délibération n° SAN-2019-001, 21 janvier 2019.

1334 Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, considérant 43 : « Pour garantir que le consentement est donné librement, il convient que celui-ci ne constitue pas un fondement juridique valable pour le traitement de données à caractère personnel dans un cas particulier lorsqu'il existe un déséquilibre manifeste entre la personne concernée et le responsable du traitement, en particulier lorsque le responsable du traitement est une autorité publique et qu'il est improbable que le consentement ait été donné librement au vu de toutes les circonstances de cette situation particulière. ».

exemple au moyen d'une déclaration écrite, y compris par voie électronique, ou d'une déclaration orale […]. Il ne saurait dès lors y avoir de consentement en cas de silence, de cases cochées par défaut ou d'inactivité ».

En matière de protection des données à caractère personnel, le caractère univoque est plus strict qu'en droit des contrats. En droit des obligations, le silence ne vaut pas acception, sauf exceptions tels que des circonstances particulières ou des relations d'affaires[1335]. En matière de protection des données à caractère personnel, il n'existe pas d'exceptions à ce principe : le silence ne vaut jamais acceptation. Le caractère univoque permet de s'assurer de la réalité du consentement[1336]. La Cour de Justice a d'ailleurs eu l'occasion de préciser que l'exigence d'une « manifestation » de volonté de la personne concernée évoque clairement un comportement actif et non pas passif : un consentement donné au moyen d'une case cochée par défaut n'implique pas un comportement actif de la part de l'utilisateur d'un site internet[1337]. Ainsi, le silence, l'inactivité ou le simple fait de continuer à utiliser un service, ne constitue en aucun cas un choix actif de la part de la personne concernée.

1335 Code civil, article 1120 : « Le silence ne vaut pas acceptation, à moins qu'il n'en résulte autrement de la loi, des usages, des relations d'affaires ou de circonstances particulières. ».

1336 Castets-Renard Céline, « Brève analyse du règlement général relatif à la protection des données personnelles », Dalloz IP/IT, 2016, 331.

1337 Cour de Justice de l'Union européenne, aff. C-673/17, 1er octobre 2019, Bundesverband c/ Planet 49, points 52 et s. : « Il apparaît pratiquement impossible de déterminer de manière objective si l'utilisateur d'un site Internet a effectivement donné son consentement au traitement de ses données personnelles en ne décochant pas une case cochée par défaut ainsi que, en tout état de cause, si ce consentement a été donné de manière informée. En effet, il ne peut être exclu que ledit utilisateur n'ait pas lu l'information accompagnant la case cochée par défaut, voire qu'il n'ait pas aperçu cette case, avant de poursuivre son activité sur le site Internet qu'il visite. » ; Document de travail des services de la Commission, analyse d'impact, annexe 2, p. 20 et pp. 105-106 : « Comme le souligne également l'avis du G29 sur le consentement, il semble essentiel de préciser que l'obtention d'un consentement valable impose de recourir à des mécanismes qui ne laissent aucun doute sur l'intention de la personne concernée de consentir au traitement, tout en expliquant que - dans le contexte de l'environnement en ligne - l'utilisation d'options par défaut, que la personne concernée doit modifier pour refuser le traitement ("consentement fondé sur le silence"), ne constitue pas, en soi, un consentement indubitable. Cela conférerait aux individus un plus grand contrôle sur leurs propres données lorsque le traitement est fondé sur leur consentement. Quant à l'incidence sur le responsable du traitement, celle-ci serait faible dès lors que cette mesure ne fait que clarifier et expliciter les implications de l'actuelle directive concernant les conditions d'un consentement valable de la part de la personne concernée. Dans la mesure où la notion de consentement "explicite" clarifierait - en remplaçant la notion de consentement "indubitable" - les modalités et la qualité du consentement et où elle ne vise pas à accroître le nombre de cas et de situations où le consentement (explicite) devrait être utilisé comme base du traitement, l'incidence de cette mesure sur les responsables du traitement ne devrait pas être majeure » ; Crichton Cécile, « Données personnelles et cases pré-cochées : toujours un défaut de consentement », Dalloz Actualité, 1 décembre 2020.

486. Un consentement éclairé. Afin de renforcer le caractère libre du consentement, le consentement doit être éclairé c'est-à-dire que l'utilisateur doit savoir à quoi il consent. Pour ce faire, le règlement européen sur la protection des données à caractère personnel renforce l'exigence de transparence[1338]. Par ailleurs, le G29 exige certaines informations minimales afin que le consentement soit caractérisé comme éclairé[1339] : le responsable de traitement doit fournir des informations comme l'identité du responsable de traitement, la finalité de chacune des opérations de traitement pour lesquelles le consentement est sollicité, les types de données collectées et utilisées, l'existence du droit de retirer son consentement etc. Le consentement doit être recueilli de manière claire et compréhensible pour chaque individu et les termes ne doivent pas être trop juridiques ou noyés dans des conditions illisibles ou interminables[1340]. L'utilisateur doit également être éclairé sur l'étendue de ses droits contenus dans le règlement européen sur la protection des données à caractère personnel.

Ainsi, le règlement européen a indubitablement renforcé la notion de consentement en précisant les caractères cumulatifs nécessaires. Dès lors, le consentement apparaît comme l'outil adéquat pour les individus afin de garder le contrôle sur leurs propres données. En réalité, l'univers numérique limite la valeur proclamée du consentement, notion surestimée en pratique.

B) La valeur surestimée du consentement

487. Réalité du consentement. Lors de l'entrée en vigueur du règlement sur la protection des données à caractère personnel, l'accent a été mis sur le pouvoir du consentement pour les individus sur leurs données. En réalité, d'une part, le consentement est concurrencé par cinq autres bases légales pour le traitement des données à caractère personnel (1). D'autre part, le consentement sur internet est amplement surestimé, voire peut avoir des effets pervers (2).

[1338] L'obligation du consentement éclairé a pour fondement l'obligation de transparence définie aux articles 12, 13 et 14 du RGPD.
[1339] Groupe de travail sur l'article 29 (G20), *op. cit.*, p. 20.
[1340] Vergnolle Suzanne, *L'effectivité de la protection des personnes par le droit des données à caractère personnel*, éd. Larcier, 2022, p. 299.

1. Une notion concurrencée

488. Une base juridique nuancée. La 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 a renforcé la place du consentement en l'érigeant comme l'une des bases juridiques possible d'un traitement de données à caractère personnel. La 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 (modifiant la Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés) est allée plus loin en érigeant le consentement comme base de référence : le consentement est une condition de référence et les cinq autres bases devenaient des dérogations à ce principe[1341]. Néanmoins, depuis l'entrée en vigueur du règlement sur la protection des données à caractère personnel, le consentement retrouve une place d'égalité avec les autres bases juridiques puisqu'il fait partie des six bases légales alternatives[1342]. Par conséquent, le règlement européen réduit la place du consentement en plaçant la notion à valeur égale parmi les autres bases juridiques.

489. Autres bases juridiques. En effet, le consentement n'est pas l'unique base juridique possible pour traiter des données à caractère personnel. Il existe cinq autres bases juridiques possibles : l'exécution d'un contrat, une obligation légale, la sauvegarde des intérêts vitaux de la personne concernée ou d'une personne physique, l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable de traitement ou

[1341] 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, article 7 : « Un traitement de données à caractère personnel doit avoir reçu le consentement de la personne concernée ou satisfaire à l'une des conditions suivantes : 1° Le respect d'une obligation légale incombant au responsable du traitement ; 2° La sauvegarde de la vie de la personne concernée ; 3° L'exécution d'une mission de service public dont est investi le responsable ou le destinataire du traitement ; 4° L'exécution, soit d'un contrat auquel la personne concernée est partie, soit de mesures précontractuelles prises à la demande de celle-ci ; 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. ».

[1342] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, article 6.1 : « 1. Le traitement n'est licite que si, et dans la mesure où au moins une des conditions suivantes est remplie : a) La personne concernée a consenti au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques. ».

encore les intérêts légitimes poursuivis par le responsable de traitement ou un tiers[1343]. Le règlement européen instaure une égalité entre les six bases juridiques possibles.

Ainsi, la notion de consentement est concurrencée par cinq autres bases juridiques. Les acteurs du numérique sollicitent le consentement comme base juridique de manière résiduelle. Pour eux, il existerait une relation contractuelle entre leurs services et les utilisateurs. En pratique, l'utilisation de cette base juridique est illicite puisque la collecte de données à des fins publicitaires n'est pas nécessaire à l'exécution du contrat[1344]. Les acteurs du numérique ne cessent d'utiliser les autres bases juridiques afin d'éviter de recueillir un consentement des utilisateurs au regard des différents caractères cumulatifs. Pour autant, le consentement peut s'avérer nécessaire afin de rendre licite certains traitements de données.

490. Base juridique ouverte. En pratique, le consentement peut également constituer *in fine* une ouverture afin de lever certaines interdictions[1345]. Par exemple, le consentement va permettre - dans certains cas - de pouvoir traiter des données sensibles[1346], de traiter des données dans une finalité incompatible[1347] ou encore d'utiliser la prise de décision fondée exclusivement sur un traitement automatisé[1348]. Dans les exemples précités, le consentement permet de lever des interdictions en faveur du responsable de traitement. Lorsqu'aucune autre base juridique est mobilisable, le consentement permet de rendre licite un traitement en principe interdit. Dès lors, les acteurs du numérique pervertissent la valeur du consentement à des fins de collecte de

1343 Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, article 6, paragraphe 1 b) à f) : « 1. Le traitement n'est licite que si, et dans la mesure où, au moins une des conditions suivantes est remplie : a) la personne concernée a consenti au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques ; b) le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci ; c) le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis; d) le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique ; e) le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement ; f) le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel, notamment lorsque la personne concernée est un enfant. ».

1344 Vergnolle Suzanne, *op. cit*., p. 282.

1345 Douville Thibault, « Le principe du consentement dans le règlement général sur la protection des données à caractère personnel », *in* Bensamoun Alexandra, Bertrand Brunessen et Anca Ailincai Mihaela (dir.), *Le règlement général sur la protection des données*, éd. Mare & Martin, 2020, p. 133.

1346 Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, article 9.1.

1347 *Ibid*., article 6 paragraphe 4.

1348 *Ibid*., article 22 paragraphe 2, c).

données des utilisateurs[1349] : le consentement permettant de rendre licite certains traitements de données dans un objectif de marchandisation[1350]. Néanmoins, les utilisateurs sont souvent incapables d'anticiper les conséquences de l'exploitation de certaines de leurs données à caractère personnel. Ils consentent aux traitements des acteurs du numérique simplement afin d'accéder au service. Dès lors, la notion du consentement libre et éclairée apparaît surestimée.

2. Une notion surestimée

491. Valeur du clic sur internet. Le consentement dans l'environnement numérique se résume souvent à un simple clic. Lorsque l'utilisateur clique sur la case « accepter », il octroie son consentement à des traitements sur des données à caractère personnel[1351]. Pour autant, le consentement de l'utilisateur doit être libre, spécifique, univoque et éclairé c'est-à-dire que l'utilisateur doit être libre de consentir, être conscient de ce qu'il accepte, connaître la finalité du traitement de ses données à caractère personnel et tout cela de manière exprès. En réalité, lors d'une simple navigation sur internet, l'internaute est confronté à une « nébuleuse de clics[1352] ». Afin d'accéder aux services, l'internaute doit accepter les conditions générales d'utilisation de chaque site souhaité. L'exemple le plus significatif étant le bandeau « cookies » affiché dès l'arrivée de l'internaute : le bandeau avertit l'internaute de la collecte de ses données et surtout lui permet de consentir ou non à cette collecte[1353], chaque clic étant censé traduire un consentement libre et éclairé. En pratique, il est facilement notable que les utilisateurs cliquent bien souvent sans avoir conscience de l'utilisation de leurs données. Pour l'utilisateur, le clic va simplement permettre de faire disparaître la bannière l'empêchant de naviguer sur internet.

1349 Netter Emmanuel, « " Refuser tous les cookies ". Espoirs et mirages d'une régulation par les boutons », Dalloz IP/IT, 2022, p. 392.

1350 Benabou Valérie-Laure et Rochfled Judith, *À qui profite le clic ?*, éd. Odile Jacob, 2015, p. 86 et s.

1351 Il s'agit par exemple de case « J'accepte que mes données soient utilisées pour recevoir des publicités personnalisées ».

1352 Cohen Dany, « Ampleur et qualités du consentement donné par clic de souris », LPA, n°164, 18 août 2014, p. 3.

1353 Netter Emmanuel, « La publicité ciblée n'est pas "nécessaire" au contrat de réseau social. Le crépuscule d'un modèle d'affaires », RTD com., 2023, p. 359.

492. « Mythologie » du consentement. Ainsi, l'absence de conséquence négative est bien souvent utopique : le refus de consentir à transmettre certaines données - généralement non indispensables à la conclusion du contrat - empêche la poursuite de la navigation[1354]. Le consentement n'est donc pas libre puisque l'utilisateur n'a pas réellement le choix. Il est alors possible d'évoquer une certaine « mythologie du consentement[1355] », c'est-à-dire l'obtention sur l'univers numérique de consentements totalement « creux[1356] » ou encore « vides[1357] ». Au final, il existe un décalage entre la promotion de l'autodétermination informationnelle et la réalité qui « apparaît de plus en plus comme une coquille vide dépourvue d'effectivité[1358] », réduisant significativement l'effectivité du principe. À titre d'illustration, la société Meta Platforms Ireland Limited (Meta Ireland) a fait l'objet de deux enquêtes par la Commission de protection des données irlandaise relative à l'absence de réel choix pour les utilisateurs[1359]. En l'espèce, les utilisateurs des services d'Instagram et de Facebook devaient accepter les conditions de service mises à jour pour pouvoir continuer d'utiliser les services de ces applications. En cas de refus, les utilisateurs perdaient l'accès à ces applications. Ainsi, les plaignants ont soulevé le fait que Meta Irland « forçait » les utilisateurs à consentir au traitement de leurs données[1360]. En réalité, ce sont les acteurs du numérique qui imposent leurs conditions à travers les

[1354] Poullet Yves « Le RGPD - une volonté de bien faire : certes ! … mais approprié ? », *in* Terwangne Cécile, Ros Karen, Poullet Yves *et al.* (dir.), *Le règlement général sur la protection des données (RGPD/GDPR),* éd. Larcier, 2018, p. 14 : « Quoi qu'il en soit, je relève que le consentement donné individuellement par la personne concernée reste bien souvent un leurre au regard de la nécessité sociale de l'accès à l'internet et à certains services (les réseaux sociaux, les moteurs de recherche, etc.) : le processus technologique interdit le recul indispensable à une bonne compréhension, à l'heure où la prétendue gratuité du service est avancée comme un bénéfice unilatéral pour la personne concernée et donc mérite en échange la possibilité pour le fournisseur du service à contenu numérique de traiter les données. » .

[1355] Koops Bert-Jaap, « The Trouble with European Data Protection Law », International Data Privacy Law, 8 October 2014, pp. 250-261.

[1356] Netter Emmanuel, « Sanction à 50 millions d'euros : au-delà de Google, la CNIL s'attaque aux politiques de confidentialité obscures et aux consentements creux », Dalloz IP/IT, 2019, p. 165.

[1357] Benabou Valérie-Laure et Rochfled Judith, *op. cit*., p. 72.

[1358] Bordais Pierre. « L'autodétermination informationnelle à l'épreuve des évolutions technologiques », Dalloz IP/IT, 72, février 2024.

[1359] Décision « Facebook », Data Protection Commission irlandaise, 31 décembre 2022, rendue publique sur le site du CEPD le 12 janv. 2023 ; Décision « Instagram » de la Data Protection Commission irlandaise du 31 décembre 2022, rendue publique sur le site du CEPD, le 12 janvier 2023 ; Décision « Facebook » du CEPD du 5 décembre 2022, rendue publique sur le site du CEPD, le 12 janvier 2023 ; Décision « Instagram » du CEPD du 5 décembre 2022, rendue publique sur le site du CEPD, le 12 janvier 2023 ; Sénéchal Juliette, « Protection des données : exclusion du contrat comme base de traitement licite aux fins de diffusion de publicités comportementales par les services numériques de réseaux sociaux », Dalloz IP/IT, 2023.

[1360] Sénéchal Juliette, *op. cit.*

conditions générales et le consentement est réduit à une adhésion aux actes unilatéraux imposés par ces acteurs[1361].

Le consentement n'illustre donc pas réellement la liberté de choix promue lors de l'entrée en vigueur du règlement sur la protection des données à caractère personnel : les utilisateurs ne savent pas réellement à quoi ils consentent. Au contraire, le consentement donne une illusion de contrôle aux utilisateurs et cette inconscience des individus sur la portée du consentement profite aux très grandes plateformes. Par ailleurs, ces acteurs du numérique développent sans cesse des nouvelles techniques de manipulation afin d'obtenir plus rapidement le consentement des internautes.

II. L'application illusoire du consentement en pratique

493. Emprise sur les utilisateurs. En pratique, les utilisateurs n'ont pas réellement conscience de la portée des traitements et renoncent à leurs droits avec un « consentement vulnérable » (A). L'absence de prise de conscience des utilisateurs constitue une aubaine pour les géants du numérique. Afin de maintenir cette emprise sur les utilisateurs, ils développent sans cesse des technologies de manipulation afin d'obtenir un « consentement superficiel » des utilisateurs (B).

A) Un « consentement vulnérable » pour les utilisateurs

494. Vulnérabilité des internautes. Au sein de l'environnement numérique, les acteurs sursollicitent les utilisateurs afin d'obtenir un « consentement vulnérable ». En effet, la vulnérabilité peut être définie comme quelqu'un ou quelque chose qui peut être atteint facilement, de par ses imperfections ou ses insuffisances[1362]. Les individus peuvent être atteints

[1361] Frison-Roche Marie-Anne, « Les conséquences régulatoires d'un monde repensé à partir de la notion de "donnée" », *in* Frison-Roche Marie-Anne et Benzoni Laurent (dir.), *Internet, espace d'interrégulation*, éd. Dalloz, 2016, p. 202 : « Dans ce système médiéval de liens entre des maîtres vers lesquels convergent les utilisateurs, ce sont les maîtres qui posent les conditions d'usage, par des conditions générales, chartes et autres engagements ou codes de conduite privés. S'il y a consentement, il se fait donc non pas par échange mais par adhésion à ces actes unilatéraux. Le Droit admet de plus en plus ce type de convergences de volonté, d'un émettant la norme commune, qui vaut cadre pour le groupe, tandis que les autres y adhèrent, le Droit laissant désormais faire tant qu'il n'y a pas d'abus. » ; Fabre-Magnan Muriel, *L'institution de la liberté*, éd. PUF, 2023.

[1362] CNRTL, v° « Vulnérable », sens 2.

facilement par les très grandes plateformes, qui font en sorte de développer la gratification immédiate pour les individus (1). La pratique de la gratification immédiate est renforcée par l'asymétrie d'information, rendant définitivement vulnérable les consentements des individus (2).

1. La gratification immédiate

495. Sursollicitation des utilisateurs. Au travers des différentes réglementations, les traitements de données à caractère personnel deviennent de plus en plus encadrés. Les responsables de traitement doivent déterminer une base légale de traitement afin de rendre licite le traitement des données. Lorsque les responsables de traitement optent pour le recueil du consentement, les caractères cumulatifs du consentement doivent être satisfaits. Pour ce faire, les individus sont sollicités par les responsables de traitement à accepter leurs conditions afin de rendre le traitement licite. Néanmoins, au regard de l'accessibilité et de l'environnement numérique, les demandes d'acceptations sont nombreuses au fil de la navigation. Cette « sursollicitation » des personnes concernées entraîne une lassitude[1363], voire une certaine résignation des personnes à l'égard de la protection de leurs propres données[1364]. Les internautes consentent de manière pratiquement automatique à la collecte de leurs données[1365]. Le fait de consentir sans réellement réfléchir nous semble pouvoir être qualifié de « consentement de vulnérable », c'est-à-dire un consentement octroyé sans réellement comprendre la portée de l'acte, simplement pour poursuivre la navigation.

496. Économie de la gratification immédiate. Les individus vont avoir tendance à accepter la collecte de leurs propres données simplement afin de pouvoir continuer leur navigation librement. La satisfaction d'accéder à un site rapidement plutôt que de comprendre l'impact de la collecte de ses données est un comportement spécifique de l'économie de la gratification immédiate[1366] : les individus sont réticents à protéger leurs données à caractère personnel en échange de récompenses relativement faibles mais immédiates. Selon le Professeur Cass Sunstein, le consentement automatique des internautes découle de trois facteurs. Le premier

[1363] Comité Européen de la Protection des Données (CEPD), « Guidelines 05/2020 on consent under Regulation 2016/679 », 4 mai 2020, paragraphe 97, p. 19.
[1364] Vergnolle Suzanne, *op. cit.*, p. 184.
[1365] Rouvroy Antoinette et Colin Jean-Noël, « Des données et des Hommes. Droits et libertés fondamentaux dans un monde de données massives », Conseil de l'Europe, 2016.
[1366] Acquisti Alessandro et Rochelandet Fabrice, « Les comportements de vie privée face au commerce électronique », La Découverte, 2011.

facteur est l'inertie des consommateurs dès lors qu'effacer ses données demande un effort, une démarche active, alors que leurs données n'ont pas forcément d'importance à leurs yeux. Le deuxième facteur résulte du fait que les internautes ont tendance à penser que la plupart des autres personnes consentent également à cette collecte et que les règles par défaut sont conçues par des experts. Enfin, les individus sont plus sensibles au risque de perdre un avantage immédiat plutôt que l'opportunité de gagner quelque chose plus tard en changeant leur comportement. Pour les individus, les services personnalisés peuvent constituer un avantage[1367]. Ainsi, les internautes acceptent de transférer leurs données à caractère personnel en l'échange de faibles récompenses, cependant immédiates. Il s'agit du phénomène de la « privacy paradox », c'est-à-dire l'échange de données à caractère personnel contre un bref gain de temps ou le bénéfice d'une fonctionnalité accessoire[1368].

497. Distorsions psychologiques. Les individus optent donc pour des avantages immédiats et présents plutôt que d'anticiper des risques : l'évaluation des éventuelles conséquences est une gestion de l'information à long terme tandis qu'accepter les traitements de données entraîne un avantage à court terme[1369]. La gestion de l'information à long terme va permettre d'évaluer des potentiels préjudices. Or, les individus sont généralement victimes de biais d'optimisme, c'est-à-dire une perception erronée que les risques sur internet concernent seulement les autres. Lorsqu'un individu poste une photo sur Facebook, il cherche à obtenir des bénéfices immédiats tels que des commentaires positifs ou des « *likes* ». Lors de la publication, l'individu va favoriser la valorisation de l'exposition personnelle et non les diverses conséquences que pourrait engendrer cette photo.

498. Rationalité limitée. La distorsion entre les bénéfices immédiats et les risques ultérieurs est également liée à une rationalité limitée des individus. En effet, pouvoir faire l'objet d'une fraude bancaire est une variable que les individus peuvent prendre en compte. En revanche, faire l'objet d'une usurpation d'identité dans plusieurs années est un risque plus difficile à identifier[1370]. Il existe une réelle difficulté pour les internautes de prendre le recul nécessaire

1367 Sunstein Cass, « Impersonal Default Rules vs. Active Choices vs. Personalized Default Rules : A Triptych », 19 mai 2013.
1368 Latil Arnaud, *Le droit du numérique : une approche par les risques*, éd. Dalloz, 2023, p. 231.
1369 Solove Daniel, « Introduction : Privacy Self-Management and the Consent Dilemma », 2013, Harvard Law Review.
1370 Acquisti Alessandro et Rochelandet Fabrice, *op. cit*.

lors du clic traduisant le consentement[1371]. Dès lors, les individus préfèrent choisir les services proposés par les plateformes au détriment de l'exploitation de leurs données, une notion encore vague pour les utilisateurs. La rationalité limitée est encouragée par les plateformes qui utilisent des techniques élaborées par des spécialistes de sciences comportementales reposant sur « l'exploitation des biais cognitifs afin de limiter la rationalité et de favoriser les actions compulsives, mues par nos émotions[1372]».

499. Absence de liberté. Récemment, Facebook avait décidé de ne plus faire dans la subtilité. La société avait mis en place un système selon lequel l'utilisateur pouvait « choisir » entre un abonnement payant ou accepter les *cookies* publicitaires. Forcément, la majorité des individus va malheureusement choisir l'option publicitaire : l'association NOYB avait rendu une étude à ce sujet démontrant que 99,9% des visiteurs acceptent le suivi lorsqu'ils sont confrontés à une redevance de 1,99 euros[1373]. L'alternative n'est pas donc pas adéquate afin de protéger les utilisateurs. Surtout, le choix binaire entre « payer ou accepter » fait douter de la validité du consentement et particulièrement du caractère libre nécessaire à un consentement valable. À propos de Facebook et à l'initiative de certaines autorités de régulation, le Comité européen de la protection des données a rendu un avis sur la conformité de cette alternative. Tout d'abord, le Comité rappelle que le consentement ne peut constituer une base légale valide que dans la mesure où la personne concernée dispose bien d'un contrôle et d'un choix réel concernant l'acceptation ou le refus des conditions proposées ou de la possibilité de les refuser sans subir de préjudice[1374]. Toutefois, le Comité considère que l'alternative binaire « payer ou accepter » n'est pas intrinsèquement illégale[1375]. L'appréciation se fera au cas par cas, en fonction de la position sur le marché du responsable de traitement, et de la dépendance des personnes au service. Il nous semble regrettable d'aboutir à des issues de plateformes soit payantes, soit

[1371] Poullet Yves, *Le RGPD face aux défis de l'intelligence artificielle*, éd. Larcier, 2020, p. 75.
[1372] Rochfeld Judith et Zolynski Célia « Quelles limites aux traitements des émotions ? », Dalloz IP/IT, décembre 2023, p. 618.
[1373] NOYB, « Pay or Okay » : 1 500 € par an pour votre vie privée en ligne ? », disponible en ligne, 19 mars 2024 ; Martial Braz Nathalie, « Meta sous tension : tirs croisés de régulation numérique ! », CCE, n° 12, décembre 2023.
[1374] Comité européen de la protection des données (CEPD), « Opinion 08/2024 on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms », 17 avril 2024.
[1375] Netter Emmanuel, « "Payer ou consentir" n'est généralement pas une alternative acceptable. Un clou de plus dans le cercueil de la publicité ciblée », RTD com., 2024, p. 337 ; Martial-Braz Nathalie. « Quand Meta se voit contraint d'abandonner la publicité ciblée sans consentement », CCE, n°12, 2023, 94.

intrusive de la vie privée. Le présent exemple démontre amplement le caractère « vulnérable » plutôt que « libre » du consentement donné par les utilisateurs sur l'environnement numérique.

Par ailleurs, les acteurs du numérique pratiquent délibérément l'asymétrie informationnelle[1376], réduisant d'autant plus la portée du consentement.

2. L'asymétrie informationnelle

500. Droit à l'information de l'utilisateur. Lorsque le responsable de traitement souhaite traiter les données des utilisateurs, il doit fournir certaines informations telles que sa propre identité, les finalités du traitement auquel sont destinées les données à caractère personnel ainsi que la base juridique du traitement ou encore les destinataires ou catégories de destinataires des données à caractère personnel[1377]. Les considérants du règlement sur la protection des données précisent que cette information doit être loyale, c'est-à-dire que les informations relatives au traitement de ces données à caractère personnel soient « aisément accessibles, faciles à comprendre, et formulées en des termes clairs et simples[1378] ». Le droit à l'information est l'une des composantes de la capabilité des individus : ils doivent comprendre la portée et l'exactitude de l'exploitation de leurs données à caractère personnel. En réalité, les individus n'ont pas réellement connaissance de l'objet de leur consentement. L'accessibilité de l'information apparaît chimérique : les informations sont imbriquées dans des conditions générales d'utilisations interminables. Le fait de « noyer » l'utilisateur est précisément le fruit d'une volonté des plateformes de lasser l'internaute avant même d'avoir commencé la lecture. En effet, la lecture de ces conditions nécessite plusieurs heures, voire des dizaines d'heures. La pratique n'est pas nouvelle, la doctrine ayant déjà soulevé cette problématique en droit de la consommation[1379]. Néanmoins, cet usage est amplifié dans l'environnement numérique en raison de l'absence d'ergonomie pour la lecture d'une telle quantité d'informations[1380]. L'absence d'information de l'utilisateur rend vulnérable le sujet du consentement.

1376 Lanna Maximilien, « Les objets connectés : entre remise en question de la notion de vie privée et évolution du droit des traitements des données personnelles », Revue de droit public n°5, 2017, p. 1435.
1377 Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, article 13 ; Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, article 32.
1378 *Ibid*., considérant 39.
1379 Temple Henri, « Le droit de la consommation est-il subversif ? », Études de droit de la consommation, Dalloz, 2004, p. 1067.
1380 Castets-Renard Céline, *Droit du marché unique numérique et intelligence artificielle,* éd. Bruylant, 2020, p. 252.

501. Vulnérabilité des individus. En effet, l'illusion de contrôle des individus sur leurs données instaure un rapport de vulnérabilité entre les plateformes et les internautes. Tout d'abord, le déséquilibre est manifeste entre les rapports de force des individus et des très grandes plateformes. La masse d'informations détenue par les acteurs du numérique permet à ces derniers de se trouver en position de force vis-à-vis des internautes. Plus les plateformes engendrent des données sur les utilisateurs, plus les internautes sont vulnérables. En réalité, il est possible de considérer que l'ensemble des individus sont vulnérables au regard du déséquilibre engendré par les technologies fondées sur les données[1381]. La vulnérabilité des individus est renforcée - de manière volontaire par les acteurs du numérique - avec l'asymétrie d'information.

502. Asymétrie informationnelle. Il existe une réelle asymétrie informationnelle entre le responsable de traitement et l'utilisateur[1382] qui s'explique par le caractère complexe et technique du droit des données à caractère personnel[1383]. En effet, les individus n'ont pas réellement connaissance de l'objet de leur consentement et l'absence d'information sur cet objet est une volonté manifeste des acteurs du numérique : l'information est rarement transmise dans des termes aisément compréhensibles. La pratique est délibérée puisque cela permet de laisser l'individu dans l'incompréhension de la réalité des traitements de ses données à caractère personnel. Lorsque l'individu est inconscient de l'exploitation de ses données, il ne pourra pas exercer ses droits[1384]. Dans le meilleur des cas, lorsque l'internaute a connaissance de potentiels traitements de ses données, il reste dans l'incertitude de savoir quelles données sont collectées, pour combien de temps et pour quelle finalité. Un individu parfaitement informé de la pratique des *cookies* publicitaires n'a pas de raison de consentir à la collecte de ses données à caractère personnel[1385].

1381 Eynard Jessica, « RGPD "empouvoirement" individuel : promesse tenue ou espoir déçu ? », RAE, 2021, p. 18.

1382 Lanna Maximilien, *op. cit*., p. 1435.

1383 Ochoa Nicolas, « Pour en finir avec l'idée d'un droit de propriété sur ses données personnelles : ce que cache véritablement le principe de libre disposition », RFDA, 2015, p. 1157.

1384 Netter Emmanuel, « À quoi sert le principe de transparence en droit des données personnelles ? », Dalloz IP/IT, novembre 2020, p. 611.

1385 Netter Emmanuel, « "Refuser tous les cookies". Espoirs et mirages d'une régulation par les boutons », Dalloz IP/IT, 2022, p. 392 : « Pourquoi révéler la liste de ses centres d'intérêt à un responsable de traitement, au risque qu'elle soit mal utilisée, revendue ou qu'elle devienne accessible aux tiers à la suite d'une faille de

Ainsi, la vulnérabilité des internautes profite aux géants du numérique. Ils développent sans cesse des pratiques permettant de recueillir un « consentement superficiel » des utilisateurs afin de pouvoir collecter toujours plus de données.

B) Un « consentement superficiel » pour les acteurs du numérique

503. Annonce de plan. Les géants du numérique vont continuellement développer des techniques novatrices afin de manipuler le consentement des utilisateurs (1). Le consentement nous semble « superficiel » puisqu'en l'absence d'obtention du consentement des utilisateurs, les acteurs du numérique disposent d'une autre base légale (2).

1. La manipulation du consentement

504. Manipulation du langage. Dans l'environnement numérique, les individus sont ordinairement inconscients de servir de « cobayes » pour des expériences de psychologie sociale tentant de manipuler leurs émotions et leurs convictions[1386]. Dans l'hypothèse où les plateformes délivreraient une information transparente telles que « vos données sont utilisées pour réaliser des profils socio-types afin de réaliser notre chiffre d'affaires en publicité ciblée », « vos données sont utilisées pour réaliser des profils socio-types afin d'influencer de futures enquêtes politiques » ou encore « ce site collecte vos données » plutôt que « ce site utilise des cookies », les individus refuseraient davantage les traitements de leurs données. En effet, il est rarissime que les plateformes soumettent explicitement le consentement des individus à des fins de profilage. Dans le meilleur des cas, l'utilisateur sera conscient de l'exploitation des données à des fins de profilage, mais restera inconscient de la technique ou du type de données exploitées[1387]. *In fine*, la communication d'une information évasive est une pratique fréquente des géants du numérique afin de récolter un consentement dit « superficiel ».

---

sécurité ? S'il est permis d'accéder au service sans s'exposer ainsi, autant dire "non" ! […] Forçant un peu le trait, on pourrait dire qu'actuellement, les services "gratuits" sont financés par les internautes qui n'ont pas compris qu'ils pouvaient entrer sans contrepartie en données personnelles. ».

1386 Rouvroy Antoinette, « Des données sans personne : le fétichisme de la donnée à caractère personnel à l'épreuve de l'idéologie des Big Data », Étude annuelle du Conseil d'État, La Documentation française, 2014, pp. 407-422.

1387 Boizard Maryline, « Le consentement à l'exploitation des données à caractère personnel : une douce illusion ? », CCE, 2016.

505. Manipulation du choix. Toujours à propos des *cookies*, les géants du numérique pratiquent également la manipulation du choix. En effet, le principe est élémentaire : refuser les *cookies* doit être aussi simple que de les accepter. À nouveau, les plateformes usent de techniques de manipulation afin d'obtenir toujours plus d'adhésion à la collecte des données. La Commission nationale de l'informatique et des libertés a condamné Microsoft à ce sujet puisque la société rendait le mécanisme de refus des *cookies* plus complexe que celui consistant à les accepter[1388]. Pour l'autorité de protection des données, cela « revient en réalité à décourager les utilisateurs de refuser les *cookies* et à les inciter à privilégier la facilité du bouton "Accepter", ce qui est renforcé par le fonctionnement même de la navigation d'Internet caractérisé par sa rapidité et sa fluidité »[1389]. En réalité, nombre de plateformes utilisent cette pratique afin de décourager l'utilisateur à refuser les *cookies*. D'autres techniques de manipulation du choix sont utilisées par les plateformes. À titre d'illustration, Facebook notifiait de fausses alertes à l'arrière du bandeau des paramètres de confidentialité afin de faire accepter plus rapidement l'utilisateur. En corrélation avec l'économie de la gratification immédiate, l'utilisateur souhaitait davantage accéder à son nouveau message plutôt que de s'attarder sur les conditions de confidentialité du groupe[1390]. En pratique, les plateformes activent par défaut les notifications afin de solliciter en continu les internautes[1391].

506. Manipulation du visuel. Par ailleurs, certaines plateformes n'hésitent pas à expérimenter le visuel afin de manipuler le choix des utilisateurs[1392]. Ils utilisent des « *dark patterns* »,

1388 Commission nationale de l'informatique et des libertés, délibération de la formation restreinte n° SAN-2022-023, 19 décembre 2022 concernant la société Microsoft ireland operations limited.

1389 Commission nationale de l'informatique et des libertés, « Cookies : sanction de 60 millions d'euros à l'encontre de Microsoft ireland operations limited », disponible sur le site de la CNIL.

1390 Braun Élisa, « Les "dark patterns" : comment les technologies nous manipulent », Le Figaro, publié le 4 juillet 2018.

1391 Pineau Karl et Fabre Aurelia, « Évaluer la captologie et le design persuasif des services numériques. Approche empirique de mesure de la persuasion et proposition d'une matrice d'évaluation », Information, données & documents, 2021, pp. 151-173.

1392 Netter Emmanuel, « "Payer ou consentir" n'est généralement pas une alternative acceptable. Un clou de plus dans le cercueil de la publicité ciblée », RTD com., 2024, p. 337 : « La suite est déjà écrite. Nous allons retrouver, sur le terrain du RGPD, les mêmes querelles déjà vues mille fois sur le terrain de la directive e-privacy, avec les bandeaux cookies : un épuisant jeu du chat et de la souris entre des autorités de protection des données qui brandiront des idéaux-types de consentement purs et parfaits, et des acteurs de terrain qui multiplieront les dark patterns et les faux dilemmes jusqu'à ce que l'internaute accepte de cliquer sur la case qui ne les privera pas de la moitié de leur chiffre d'affaires. ».

pouvant être traduit en français par « interfaces truquées » ou « interfaces trompeuses »[1393]. Le Règlement (UE) 2022/2065 du 19 octobre 2022 du Parlement européen et du Conseil relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (règlement sur les services numériques) définit ce terme comme une interface digitale qui « trompe, manipule, altère ou entrave substantiellement la capacité des utilisateurs à prendre des décisions libres et éclairées », en raison de son « design, de son organisation ou de la façon dont elle est opérée[1394] ». Il s'agit de tromperie ou de manipulation au travers d'interfaces digitales[1395]. Par exemple, certaines plateformes vont demander à l'utilisateur de cocher une case pour ne pas s'abonner à la *newsletter* et l'internaute va cocher la case en pensant légitimement faire le contraire. Selon certains chercheurs, il suffirait de faire croire que l'individu dispose d'une liberté de choix pour qu'il consente à l'exploitation de ses données à caractère personnel[1396]. Lorsque la plateforme ajoute une phrase telle que « vous êtes libres d'accepter ou de refuser », la simple évocation de la liberté suffit à anéantir le réflexe de méfiance des internautes[1397].

507. Manipulation des couleurs. D'autres plateformes manipulent les couleurs afin d'influencer le choix des utilisateurs. Il peut s'agir d'utiliser des couleurs vives afin d'insérer le bouton « Accepter » et « Refuser » de la même couleur : lorsque les deux boutons sont en vert, cela consiste à faire croire à l'utilisateur qu'il refuse alors qu'il accepte le dépôt de *cookies*

1393 *Ibid.* ; Lacombe César, « Pour une approche spatiale du numérique : repenser le design numérique », Management des technologies organisationnelles, 2021, pp. 35-50 : « Ils sont définis comme "les cas où les designers utilisent leurs connaissances du comportement humain (par exemple, la psychologie) et les désirs des utilisateurs finaux pour mettre en œuvre des fonctionnalités trompeuses qui ne sont pas dans le meilleur intérêt de l'utilisateur". La connaissance sur le cerveau humain progresse, et la connaissance de ses faiblesses progresse conjointement. Les designers UX et UI utilisent désormais cette connaissance pour tromper l'utilisateur, et lui faire réaliser des actions qui vont dans l'intérêt des plateformes et non pas dans son intérêt, ce qui est pourtant à la racine de la discipline d'UX Design et des démarches centrées utilisateurs. » ; Commission nationale de l'informatique et des libertés, « La forme des choix. Données personnelles, design et frictions désirables », Cahiers IP Innovation et prospective, 2019, n° 06, définition : « des éléments et mécanismes mis en place dans les interfaces pour influencer les décisions des utilisateurs dans un sens qu'ils ne choisiraient pas nécessairement s'ils étaient en face d'une interface loyale et transparente ».

1394 Règlement (UE) 2022/2065 du 19 octobre 2022 du Parlement européen et du Conseil relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (règlement sur les services numériques), article 25.

1395 Potel-Saville Marie « Dark Patterns : l'étau législatif se resserre (enfin ?) sur les interfaces manipulatrices ou trompeuses », RPPI, n° 2, novembre 2022.

1396 Pascual Alexandre, Guéguen Nicolas, « La technique du "vous êtes libre de… " : induction d'un sentiment de liberté et soumission à une requête ou le paradoxe d'une liberté manipulatrice », Revue internationale de psychologie sociale, 2002.

1397 Commission nationale de l'informatique et des libertés, « La forme des choix. Données personnelles, desing et frictions désirables », *op. cit.*

sur son terminal[1398]. Le fait d'utiliser des couleurs vives plutôt que des couleurs grisâtres permet d'obtenir un consentement biaisé[1399]. Il peut également s'agir d'insérer le bouton « Refuser » tout en haut à droite dans un format presque illisible afin que l'utilisateur clique sur le bouton le plus voyant, c'est-à-dire le bouton « Accepter ». Pour les membres du groupe de travail, les situations de manipulation du visuel doivent être appréciées au cas par cas : seule la pratique qui rend le texte illisible doit être qualifiée comme manifestement trompeuse[1400]. Il nous semble nécessaire de prendre en compte les autres techniques afin de protéger effectivement les utilisateurs.

508. Manipulation des sentiments. Afin de renforcer le vice de la manipulation, les géants du numérique investissent dans les sciences cognitives afin de biaiser le consentement des internautes[1401]. En effet, les plateformes disposent d'ingénieurs, de designers et de spécialistes de sciences comportementales au sein de leurs équipes. Ils sont chargés d'identifier les émotions et de les « travailler » afin d'orienter le comportement des individus concernés dans un sens désiré par le « capteur »[1402]. Pour ce faire, les plateformes utilisent des « *nudges* », c'est-à-dire des techniques d'incitation ou d'influence afin de modifier le comportement des internautes[1403]. Les *nudges* vont manipuler les choix des internautes vers des actions considérées comme positives. Les techniques utilisées par les acteurs du numérique entraînent des biais

1398 Comité européen de la Protection des données (CEPD), « Lignes directrices sur les interfaces truquées dans les interfaces des plateformes de médias sociaux », 2022 : « Les interfaces truquées sont des interfaces et des expériences utilisateur mises en œuvre sur les plateformes de médias sociaux qui amènent les utilisateurs à prendre des décisions involontaires, non désirées et potentiellement préjudiciables en ce qui concerne le traitement de leurs données à caractère personnel. Cela influence le comportement des utilisateurs et leur capacité à protéger efficacement leurs données à caractère personnel. ».

1399 Netter Emmanuel, « À quoi sert le principe de transparence en droit des données personnelles ? », Dalloz IP/IT, novembre 2020, p. 611.

1400 Comité européen de la protection des données (CEPD), « Report ont Cookie Banner Task Force », 17 janvier 2023 ; Commission nationale de l'informatique et des libertés, « Le CEPD adopte le rapport final de la « task force », dédiée aux bannières cookies » : « Les autorités s'accordent à considérer qu'elles ne peuvent imposer à tous les sites web un standard en termes de couleur ou de contraste. Un examen au cas par cas de la bannière doit être effectué pour déterminer si le design choisi (ex. couleur/contraste) n'est pas manifestement trompeur pour les utilisateurs. ».

1401 Latil Arnaud, *Le droit du numérique : une approche par les risques*, éd. Dalloz, 2023, p. 229.

1402 Rochfeld Judith et Zolynski Célia « Quelles limites aux traitements des émotions ? », Dalloz IP/IT, décembre 2023, p. 618.

1403 Fourcade Marion, « La mouche et le traqueur : alignement et désaxement dans le capitalisme au XXIe siècle », Regards croisés sur l'économie, pp. 114-125 ; Haas Gégard et Astier Stéphane, « Les biais de l'intelligence artificielle : quels enjeux juridiques ? », Dalloz IP/IT, 2019 : « Les nudges visant à modifier les biais humains sont utilisés par les services marketing pour faciliter la compréhension du consommateur à travers la vulgarisation du message ou encore attirer l'attention du consommateur. ».

cognitifs pour les utilisateurs, c'est-à-dire « des pensées illogiques, irrationnelles, générées par le contexte dans lequel est immergé l'utilisateur[1404] ». Pour les Professeures Judith Rochfled et Célia Zolynski, il s'agit de l'exploitation des émotions par des technologies de « captologie »[1405]. L'intérêt des plateformes est d'influencer les internautes afin qu'ils exercent des actions irrationnelles : il s'agit de limiter la rationalité afin d'emporter les individus vers des actions impulsives**.** Lorsque les individus sont influencés par des biais cognitifs, ils auront tendance à accepter le traitement de leurs données à caractère personnel[1406]. Les géants du numérique investissent dans ces techniques de manipulation afin de maximiser leurs revenus publicitaires[1407].

509. Manipulation technique. Pire encore, certaines plateformes n'hésitent pas à simplement se soustraire à l'obligation de recueil du consentement des utilisateurs. Par la technique, ces plateformes déposent automatiquement des *cookies* sur l'équipement terminal de l'utilisateur avant toute action de leur part[1408]. Il s'agit d'une manipulation technique pour l'utilisateur inconscient de cette manœuvre des plateformes. À ce sujet, la Commission nationale de l'informatique et des libertés a déjà condamné les sociétés « Google LLC » et « Google Ireland Limited » pour ces pratiques de manipulation[1409]. La société « Voodoo » a également été condamnée pour cette manipulation technique puisque lorsque l'utilisateur utilisait l'application Voodoo, son consentement était sollicité pour que la société puisse suivre ses activités à des fins publicitaires. Or, la Commission nationale de l'informatique et des libertés a soulevé le fait qu'en cas de refus de l'utilisateur, les traceurs continuaient d'être utilisés[1410]. L'ensemble de ces pratiques démontre que les géants du numérique se soustraient de leurs obligations, de manière délibérée et impactent les droits et libertés des individus.

1404 Groffe-Charrier Julie, « La loi est-elle dictée par le code ? », Dalloz IP/IT, 2020, pp. 602-606.

1405 Rochfled Judith et Zolynski Célia, « La valeur des émotions : quel régime pour le "capitalisme mental" ? », *Mélanges en l'honneur de Pierre Sirinelli*, éd. Dalloz, 2022, p. 764.

1406 Zolynski Célia, Le Roy Marylou et Levin François, « L'économie de l'attention saisie par le droit », Dalloz IP/IT, 2019, p. 614.

1407 Toledano Joëlle, *GAFA : Reprenons le pouvoir*, éd. Odile Jacob, 2020 p. 15.

1408 Commission nationale de l'informatique et des libertés, délibération n°SAN-2020-012, 7 décembre 2020, paragraphe 68 : « En l'espèce, les membres de la délégation ont constaté dans le cadre du contrôle en ligne du 16 mars 2020 que, lors de l'arrivée sur le site web [...].fr, sept cookies ont été déposés sur leur équipement terminal, avant toute action de leur part. Dans son courrier du 30 avril 2020, la société Y a indiqué que quatre de ces sept cookies poursuivent une finalité publicitaire. »

1409 Commission nationale de l'informatique et des libertés, n°SAN-2020-012, 7 décembre 2020.

1410 Commission nationale de l'informatique et des libertés, n°SAN-2022-026, 29 décembre 2022.

Les géants du numérique manipulent les utilisateurs par des pratiques douteuses afin d'obtenir un consentement superficiel. Toutefois, lorsque l'obtention du consentement apparaît excessivement contraignante, les acteurs disposent d'une base légale alternative : l'intérêt légitime.

2. L'alternative de l'intérêt légitime

510. Alternative équivalente au consentement. L'intérêt légitime constitue l'une des six bases légales prévues par le Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données. En principe, le responsable de traitement peut se baser sur l'intérêt légitime pour traiter des données à caractère personnel. Pour ce faire, le responsable de traitement doit opérer une mise en balance entre les « intérêts ou libertés et droits fondamentaux des personnes » et intégrer les « attentes raisonnables » de ces personnes[1411]. Ainsi, le responsable de traitement doit prendre en compte le degré d'intrusion du traitement envisagé dans la sphère individuelle, les incidences sur la vie privée des personnes concernées, etc. L'ancien groupe de travail G29 estime que l'intérêt légitime correspond à « l'enjeu poursuivi par le responsable de traitement, ou le bénéfice qu'il tire du traitement[1412] ». La Cour de Justice a même considéré que l'intérêt légitime pour un moteur de recherche pouvait être son intérêt économique, c'est-à-dire la recherche de profit par la collecte et l'utilisation des données à caractère personnel de ses utilisateurs[1413]. L'intérêt légitime pour les plateformes peut être la monétisation des informations sur leurs utilisateurs[1414]. En effet, les plateformes ont un intérêt très légitime à collecter le plus d'informations sur leurs utilisateurs pour affiner les profils et les rendre plus attractifs économiquement[1415].

1411 Commission nationale de l'informatique et des libertés, « L'intérêt légitime : comment fonder un traitement sur cette base légale ? », 2 décembre 2019, disponible sur : https://www.cnil.fr/fr/les-bases-legales/interet-legitime.

1412 G29, « Avis 06/2014 sur la notion d'intérêt légitime poursuivi par le responsable de traitement au sens de l'article 7 de la directive 95/46/CE », WP 217, 9 avril 2014, p.55.

1413 Cour de Justice de l'Union européenne (CJUE), aff. C-131/12, Google SPain SL, Google Inc. c/ Agencia Espanola de Proteccion de Datos, Mario Costeja Conzalez, 13 mai 2014, points 80 et s.

1414 Mattatia Fabrice, « Pour en finir avec le mythe du consentement RGPD », JCP, n° 16, 2020.

1415 Martial-Braz Nathalie, « Quant Meta se voit contraint d'abandonner la publicité ciblée sans consentement », CCE, n° 12, décembre 2023.

511. Une alternative potentiellement dangereuse. Par conséquent, l'intérêt légitime est utilisé par les géants du numérique afin de justifier certains traitements de données à caractère personnel. À titre d'illustration, Facebook estime se fonder sur ses « intérêts légitimes ou ceux d'un tiers » pour traiter des données, afin de « promouvoir des produits et lancer notre marketing direct ». Cette société utilise également l'intérêt légitime afin de promettre des améliorations sur l'expérience utilisateur[1416]. Les promesses servent finalement à retenir l'utilisateur le plus longtemps possible sur la plateforme afin de collecter davantage de données[1417] et d'expérimenter la manipulation des émotions.

Pour d'aucuns, cette base légale de traitement constitue une « porte ouverte[1418] » ou encore un véritable « cheval de Troie[1419]» légitimant tout traitement et permettant « de s'y référer automatiquement ou d'en élargir indûment l'utilisation au prétexte qu'il semble moins contraignant que les autres motifs[1420] ». En effet, il paraît légitime pour les géants du numérique de rechercher un intérêt économique dans les traitements des données à caractère personnel de ses utilisateurs puisque l'exploitation des données constitue leur modèle d'affaire. Pourtant, le CEPD semble condamner le recours à cette base légale puisque les atteintes sur les droits des personnes concernées sont fondées en raison de « l'extrême puissance intrusive des procédés de ciblage publicitaire »[1421]. La solution du Comité était nécessaire puisque la base légitime de traitement « annule » les effets protecteurs instaurés par le règlement sur la protection des données à caractère personnel.

1416 Vergnolle Suzanne, *L'effectivité de la protection des personnes par le droit des données à caractère personnel*, éd. Larcier, 2022, p. 277.

1417 Rouvroy Antoinette, « L'homo juridicus est-il soluble dans les données ? », *Droit, normes et libertés dans le cybermonde,* éd. Larcier, 2018, p. 436.

1418 G29, « Avis 06/2014 sur la notion d'intérêt légitime poursuivi par le traitement des données au sens de l'article 7 de la directive 95/46/CE », WP 217, 9 avril 2014, pp. 5 et 55.

1419 Martial-Braz Nathalie, Rochfeld Judith, Gattone Emilie, « Quel avenir pour la protection des données à caractère personnel en Europe ? Les enjeux de l'élaboration chaotique du règlement relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données », Dalloz, 2013, chronique 2788.

1420 G29, *op. cit*., p. 3.

1421 Netter Emmanuel, « La publicité ciblée n'est pas « nécessaire » au contrat de réseau social. Le crépuscule d'un modèle d'affaires », RTD com, 2023, p. 359 ; G29, Avis 06/2014 sur la notion d'intérêt légitime poursuivi par le responsable du traitement des données au sens de l'article 7 de la directive 95/46/CE.

512. Conclusion de la section. L'effectivité des normes s'apprécie en fonction du degré de réalisation dans les pratiques sociales. Lors de l'entrée en vigueur du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, le consentement a été promu comme l'instrument idéal permettant aux individus de contrôler l'exploitation de leurs données. Par cet outil, les individus détiendraient le choix et la maîtrise de leurs données sur les futurs usages.

L'étude du consentement démontre au contraire une absence concrète de choix libre et éclairé des individus sur l'exploitation de leurs données. L'illusion du consentement résulte d'une détermination des sociétés privées qui exploitent les données. La plupart des sociétés du numérique ont bâti leur empire sur l'exploitation des données des utilisateurs. Ainsi, l'aspiration de ces acteurs est d'obtenir le consentement des utilisateurs dans le dessein de pérenniser leurs pratiques. La masse d'informations détenues par les plateformes sur les utilisateurs place les individus dans une situation vulnérable : ils consentent aux traitements de leurs données à caractère personnel sans avoir conscience des impacts sur leur vie privée. Le consentement donné par les individus nous semble être un « consentement vulnérable » au regard de la position de force des entreprises vis-à-vis des individus et de l'asymétrie d'information.

De surcroît, afin de parvenir le plus promptement à obtenir le consentement des utilisateurs, les géants du numérique manipulent les personnes concernées. Pour ce faire, ils développent des techniques novatrices permettant de manipuler le visuel, le langage et surtout nos émotions. Les plateformes investissent dans les sciences cognitives afin de manipuler directement les sentiments des utilisateurs. Ainsi, l'unique objectif des plateformes est d'obtenir un « consentement superficiel » des individus pour faire prospérer l'exploitation de leurs données. Dès lors, l'effectivité du consentement est fortement limitée par leurs pratiques de manipulation : le consentement devient une base juridique fragile et fragilisée par les technologies émergentes.

Section 2 : Les principes de protection face à la réalité technologique

513. Renforcement des principes. Afin de renforcer la protection des données à caractère personnel pour les individus, le Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données a renforcé les principes incombant aux responsables de traitement. La protection de ces données est désormais gouvernée par des principes fondamentaux tels que le principe de minimisation ou le principe de finalité. Le dessein de ces principes est de responsabiliser les acteurs du numérique afin de protéger effectivement les personnes concernées.

514. Annonce de plan. La responsabilité renforcée des responsables de traitement permet *a priori* de protéger effectivement les utilisateurs contre les dérives des technologies émergentes. La société postmoderne est une société de données où le développement du *Big Data* devient une opportunité. En réalité, l'exploitation du *Big Data* détourne les principes de protection institués par le règlement (I). En effet, l'écart entre les principes promus et la réalité technologique entraîne des risques pour les utilisateurs, souvent inconscients du manque d'effectivité des principes de protection (II).

I. L'inadéquation des principes de protection à l'ère du *Big Data*

515. L'opposition des principes. Les caractéristiques des *big data* entrent en opposition avec les principes de protection. Le *Big Data* promet une collecte maximale des données et le principe de minimisation, son contraire. Le principe de finalité est également mis à mal par le développement de la collecte par défaut. Ainsi, les principes protecteurs sont altérés par l'expansion du *Big Data* (A). L'altération de la protection entraîne inévitablement un recul de la protection pour les individus (B).

A) L'expansion du phénomène

516. L'inadéquation des principes. Afin de comprendre l'inadéquation des principes de protection à l'ère du *Big Data*, il convient de comprendre son essor (1) et les outils nécessaires pour l'analyse de cette masse de données (2).

1. L'essor des opportunités du *Big Data*

517. L'essor de la masse de données. Les opportunités du *Big Data* sont en corrélation avec l'augmentation des données disponibles. Tout d'abord, l'essor des objets connectés participe à ces nouvelles opportunités : les objets connectés permettent une collecte massive de données puisque les capteurs sont directement intégrés au sein des objets de la vie quotidienne[1422]. Il s'agit d'une innovation technique permettant de mettre en réseau des objets physiques. De fait, les objets connectés collectent et stockent toutes ces données à des fins d'analyses[1423]. Ils font désormais partie de la vie des individus qui deviennent la source directe de ces données. À l'échelle mondiale, le nombre d'objets connectés doublerait entre 2020 et 2030 passant de 20 à 45 milliards[1424].

518. Raffinement des outils d'analyses. L'usage des outils du *Big Data* permet d'analyser la masse de données disponible et donne la possibilité aux sociétés de développer de nouveaux services personnalisés et par conséquent, de maximiser davantage leurs revenus. Le phénomène du *Big Data* offre des opportunités uniques pour les opérateurs économiques par l'analyse prédictive, l'analyse des sentiments ou encore la connaissance affinée des comportements[1425]. Par exemple, le phénomène du profilage n'est pas un phénomène nouveau. En revanche, les

[1422] Pucheral Philippe, Rallet Alain, Rochelandet Fabrice, Zolynski Célia, « La Privacy by design : une fausse bonne solution aux problèmes de protection des données personnelles soulevés par l'Open data et les objets connectés ? », Legicom, n° 56, Victoires éditions, 2016.
[1423] Lanna Maximilien, « Les objets connectés : entre remise en question de la notion de vie privée et évolution du droit des traitements des données personnelles », RDP, 2017, n° 5, p. 1435.
[1424] Béguin-Faynel Céline, « Assurances et nouvelles technologies - Objets connectés et appréciation du risque », Responsabilité civile et assurances, n° 3, mars 2023.
[1425] Zolynski Célia, « Big data : pour une éthique des données », Information, données & documents, 2015.

outils du *Big Data* et particulièrement l'intelligence artificielle modifient les modalités et la portée du profilage. Avec les capacités de stockage et d'analyse, l'Internet des objets et la multiplication des services disponibles, les quantités de données collectées sont démesurées. Les opportunités du Big Data résident dans l'utilisation d'algorithmes toujours plus puissants afin d'analyser cette quantité de données[1426].

2. Les outils d'analyse de données

519. ***Data mining***. Avec la massification des données et les traces laissées par les individus, les outils d'analyse de données vont permettre de s'affranchir de la notion de statistique traditionnelle de « moyenne »[1427]. Le *data mining*, « forage de données » ou encore « fouille de données » est un processus quasiment automatique, contrairement aux statistiques traditionnelles. Le *data mining* est une méthode d'exploration des données : il ne s'agit plus de constater une catégorie statistique dans ce qui transparait dans la masse de données mais de déduire ce qui n'apparaît pas quasiment en temps réel[1428]. Les progrès de la technologie vont permettre de substituer les statistiques classiques par la singularité des comportements humains.

En effet, la logique passe d'une logique déductive à une logique inductive : la logique inductive permet de collecter un maximum de données pour exploiter les corrélations au contraire de la logique déductive dont les conclusions se reposent sur des causalités. Les corrélations vont ensuite permettre d'extraire de nouvelles informations à des fins d'analyse prédictive[1429]. Dès lors, les d'algorithmes sont appelés « modèles prédictifs » ou encore « *patterns* »[1430]. Les modèles vont servir aux entreprises afin de passer d'un marketing de masse à un marketing personnalisé[1431]. La fouille de données devient donc une pratique indispensable aux entreprises afin d'être plus performantes sur un marché donné. En pratique, les acteurs du numérique ont utilisé excessivement le processus de *data mining* en matière d'intelligence artificielle

[1426] Poullet Yves, « Cinq ans après : le RGPD et les défis du profilage à l'heure de l'intelligence artificielle », RAE, 2021, p. 88 : « Les systèmes d'information actuels par leur interactivité, leur interconnexion et leur ubiquité permettent d'élargir - et ce de manière exponentielle - le nombre de données collectées et traitées. ».
[1427] Brasseur Christophe, *op. cit*.
[1428] Bougeard Aurélien, « Le phénomène de Big Data et le Droit, Pour une appréhension juridique par sa décomposition technique », Thèse, Strasbourg, p. 88.
[1429] Zolynski Célia, *op. cit.*
[1430] Rouvroy Antoinette, *op. cit.*
[1431] Basdevant Adrien et Mignard Jean-Pierre, *L'empire des données*, éd. Don Quichotte éditions, 2018, p. 59.

générative. Le *data mining* met en lumière l'enjeu fondamental de protection des données à caractère personnel dans le développement de l'intelligence artificielle[1432].

520. ***Machine learning***. Le *machine learning* ou apprentissage automatique correspond à un sous-ensemble des techniques de *data mining*, les deux techniques étant complémentaires. Le *machine learning* va permettre aux machines d'évoluer grâce à un processus d'apprentissage. Il existe différents modes d'apprentissage : supervisé ou non supervisé. L'apprentissage est supervisé lorsque l'algorithme est entrainé avec des données prévues par un superviseur humain. Les données contiennent à la fois les données nécessaires et les résultats attendus. L'algorithme est dit supervisé lorsque l'humain valide ou réajuste l'algorithme en fonction des attentes. Au contraire, l'apprentissage non supervisé n'est pas entrainé avec des données prévues par l'humain mais simplement avec un jeu de données. L'algorithme doit ensuite analyser les données et relever des corrélations afin d'identifier des modèles sous-jacents. Le modèle non supervisé va produire des résultats inattendus, imperceptibles à l'œil humain[1433]. L'objectif étant d'extraire des *patterns* ou des régularités non prescrites par avance. Il s'agit de « l'émergence progressive, au cours de fonctionnement du réseau, de catégories ou de classes nouvelles, auxquelles l'humain n'aurait pas pensé, ou pu découvrir, en raison des limites de ses capacités d'analyse ou de perception »[1434]. À la différence du *data mining*, l'objectif final du *machine learning* est de rendre la machine entièrement autonome.

521. ***Deep learning***. Le *deep learning* ou apprentissage en profondeur utilise des algorithmes complexes de réseaux de neurones profonds inspirés du fonctionnement du cerveau humain[1435]. La technique du *deep learning* peut être définie comme un « traitement effectué par un grand nombre de neurones artificiels (imitant de façon très simplifiée les neurones biologiques) qui, par leurs interactions, permettent au système d'apprendre progressivement à partir d'images, de textes ou d'autres données. L'apprentissage repose sur des principes mathématiques généraux. Le résultat de l'apprentissage est une représentation, une décision ou une transformation[1436]. Au final, les termes de *machine learning* et de *deep learning* se retrouvent

---

1432 Jeulin Betty, « Amendement de l'Artificial Intelligence Act : la théorie confrontée à la pratique », Dalloz Actualité, 14 juin 2023.

1433 Rouvroy Antoinette et Colin Jean-Noël, « Des données et des hommes. Droits et libertés fondamentaux dans un monde de données massives », 2016, p. 14.

1434 V. Lambert Dominique, *La robotique et l'intelligence artificielle*, Paris, éd. Lessius, 2019.

1435 Deltorn Jean-Marc, « La protection des données personnelles face aux algorithmes prédictifs », Revue des droits et libertés fondamentaux, 2017.

1436 Barra Vincent, « Apprentissage automatique et réseaux de neurones », Tangente, hors-série n°68, octobre 2018, pp. 44-47.

dans le terme d'intelligence artificielle. En revanche, le phénomène est source de risques majeurs pour les individus lorsque le développement de ces technologies émergentes se réserve à quelques acteurs dominants[1437].

B) Le recul de la protection

522. Antinomie des principes. Les principes protecteurs du règlement sont en totale inadéquation avec les principes du *Big Data*. En effet, les principes de finalité, de minimisation (1) ou encore le principe d'effacement des données sont simplement antinomiques aux caractères du *Big Data* (2). L'inadéquation des principes au phénomène de massification des données entraîne *de facto* un recul de la protection des individus.

1. Les limites des principes de finalité et de minimisation

523. Principe de finalité. Le principe de finalité est un principe fondamental pour la protection des données à caractère personnel. La Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés précise que les données à caractère personnel doivent être « collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités[1438] ». Il s'agit d'anticiper et surtout d'interdire les collectes de données sans finalité déterminée : l'utilisateur doit être conscient de la finalité de la collecte de ses données à caractère personnel[1439]. Le principe de finalité répond aux objectifs suivants : un impératif de transparence, un impératif de prévisibilité et surtout un impératif de sécurité juridique[1440]. Grâce à ces différents impératifs, la personne concernée est informée de la finalité du traitement et de son étendue, ce qui lui permet de contrôler l'usage de ses données. Ainsi, lorsque le traitement ultérieur est incompatible avec la finalité initiale, le traitement est simplement interdit.

524. Limites du principe de finalité. En réalité, le principe de finalité entre en opposition frontale avec le principe des données massives. Le principe de finalité est un principe qui

[1437] Laneret Nathalie, « L'accountability et la protection effective des données personnelles dans un monde digital connecté », RUE, n° 634, 2020, pp. 35-40.
[1438] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, article 6, 2°.
[1439] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, considérant 42.
[1440] Groupe de travail sur l'article 29 (G29), Avis n°03/2013 sur le principe de finalité, 00569/13/EN, WP 203, adopté le 2 avril 2013.

s'applique à des traitements « figés » alors que le *Big Data* repose sur des traitements évolutifs et dynamiques[1441]. En effet, la valeur des *big data* repose précisément sur ses utilisations secondaires, c'est-à-dire des exploitations encore inconnues lors de la collecte. Les corrélations que vont découvrir les algorithmes peuvent amener le responsable de traitement à utiliser les données à d'autres fins que celles initialement prévues[1442]. La nature évolutive du phénomène empêche une prévisibilité et donc une détermination de sa finalité[1443].

525. Nature évolutive des traitements. En pratique, le phénomène du *Big Data* a pour objectif de maintenir les données dans les systèmes d'information afin de pouvoir « nourrir » les algorithmes et les entraîner. Les traitements algorithmiques vont exploiter indifféremment des données à caractère personnel et des données à caractère non personnel[1444]. De plus, les données peuvent avoir des finalités extrêmement variées lors de leur exploitation : certaines données seront collectées pour une finalité déterminée et pourront être utilisées à d'autres fins non prévues initialement[1445]. Les systèmes de *machine learning* fonctionnent grâce à des corrélations statistiques établies sur des rapprochements qui ne sont pas forcément prévisibles. En effet, le potentiel des données peut se manifester en cours de route grâce aux outils du *Big Data*[1446]. Surtout, il serait contraire au développement des données massives de supprimer les données une fois leur finalité utilisée. Le plus complexe sera alors de déterminer quels sont les acteurs ayant traité ces données. Ainsi, le principe de finalité est contraire à la nature même des données massives, qui privilégie les usages secondaires[1447].

526. Principe de minimisation. Par ailleurs, le principe de minimisation est le corollaire du principe de finalité. En effet, le principe de minimisation prévoit que les données à caractère personnel doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des

---

1441 De Terwangne Cécile, « Principes de base de la protection des données », *in* Rosir Karen (dir.), *Le règlement sur la protection des données. Analyse approfondie*, éd. Larcier, p. 84 : « [l]'interdiction de traitement en cas d'incompatibilité des finalités s'oppose à l'évolution d'un traitement de données qui est en quelque sorte "figé" par sa finalité réelle de départ. ».

1442 Toledano Joëlle, *GAFA : Reprenons le pouvoir,* éd. Odile Jacob, 2020, p. 64.

1443 Bensamoun Alexandra et Zolynski Célia, « Cloud computing et big data », La Découverte, 2015, p. 7.

1444 Warusfel Bertrand, « Régulation du numérique et souveraineté dans le cyberespace », Dalloz IP/IT, 2022, pp. 547-551.

1445 Vergnolle Suzanne, *L'effectivité de la protection des personnes par le droit des données à caractère personnel*, éd. Larcier, 2022, p.175.

1446 Rouvroy Antoinette, « L'homo juridicus est-il soluble dans les données ? », *in* Poullet Yves (dir.), *Droit, normes et libertés dans le cybermonde,* éd. Larcier, 2018, p. 436.

1447 Bensamoun Alexandra et Zolynski Célia, *op. cit*.

finalités pour lesquelles elles sont traitées[1448] : les données ne doivent donc pas être excessives et strictement limitées à la finalité déterminée. À nouveau, ce principe entre également en opposition avec la nature même du principe des *Big Data*. Les données massives sont - au contraire du principe de minimisation - un principe de collecte maximale, automatique, par défaut[1449]. Le principe de minimisation serait « le témoin privilégié de l'incompatibilité » entre le Big Data et les principes protecteurs[1450].

527. Collecte en excès des données. Par conséquent, les responsables de traitement vont privilégier une collecte maximale afin de pouvoir faire apparaître des profils, des catégories ou des modèles prédictifs : il s'agit d'une véritable mine d'or future pour les responsables de traitement[1451]. Les responsables de traitement ont tendance à conserver les données en excès afin de faire ressortir la valeur des données[1452]. Plus le responsable de traitement détient de données, plus l'agrégation pourra être source de valeur. Ainsi, la conservation des données en excès limite le principe de minimisation et par conséquent, la protection des personnes concernées sur leurs données à caractère personnel. Afin de contrer ces pratiques, les utilisateurs bénéficient d'un droit à l'effacement. En réalité, ce droit est également mis à mal par les technologies utilisées pour traiter les données massives.

1448 CNIL, Définition minimisation ; Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, article 5.

1449 Rouvroy Antoinette, « La robotisation de la vie et la tentation de l'inséparation », *in* Jacquemin Hervé et De Streel Alexandre (dir.), *L'intelligence artificielle et le droit*, éd. Larcier, 2017, p. 23 : « La prolifération et le traitement de quantités massives de données - présupposés par le phénomène des Big Data et par les outils robotiques qui s'en nourrissent - entrent en opposition frontale avec les grands principes de protection des données : la minimisation (on ne collecte que les données nécessaires au but poursuivi), la finalité (on ne collecte de donnée qu'en vue d'un but identifié, déclaré légitime), la limitation dans le temps (les données doivent être effacées une fois le but atteint et ne peuvent être utilisées, sauf exceptions, à d'autres fins que les fins initialement déclarées. Les Big Data c'est au contraire une collecte maximale, par défaut, la conservation illimitée de tout ce qui existe sous une forme numérique, sans qu'il y ait nécessairement de finalité établie a priori, puisque l'utilité des données ne se manifeste qu'en cours de route, à la faveur des pratiques statistiques de datamining, de machine learning, etc. ».

1450 Laroche Benjamin, « Le big data à l'épreuve du règlement européen sur la protection des données », Thèse, Toulouse, 2020, p. 158.

1451 Vergnolle Suzanne, *op. cit.*, p. 375.

1452 Rouvroy Antoinette et Colin Jean-Noël, *op. cit.*, p. 29 : « Dans la mesure où, comme expliqué plus haut, l'utilité réelle d'une donnée - y compris une donnée à caractère personnel - dépend de la quantité des autres données récoltées avec lesquelles elle pourrait être agrégée, les responsables de traitement ont nécessairement tendance à les conserver non seulement lorsqu'elles sont utiles ou nécessaires à la fourniture d'un service déterminé, mais aussi en excès de ce qui serait strictement nécessaire aux services dont ils gratifient leur clientèle. ».

2. Les limites du droit à l'effacement

528. Principe du droit à l'effacement. Dans le dessein de résister aux pratiques néfastes pour la protection des données à caractère personnel, les personnes concernées disposent d'un droit à l'effacement : ils ont la possibilité d'obtenir du responsable de traitement l'effacement, dans les meilleurs délais, des données à caractère personnel les concernant. Le responsable de traitement a l'obligation d'effacer ces données à caractère personnel. Plusieurs motifs sont évoqués : lorsque les données à caractère personnel ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées d'une autre manière ou lorsque la personne concernée retire simplement le consentement sur lequel est fondé le traitement[1453]. Lors de l'analyse de ce principe, un paradoxe peut être soulevé : lorsque la personne concernée n'a pas été informée de la finalité du traitement, dans quelle mesure peut-elle demander la suppression de ses données sur le fondement de ce motif. Au-delà, il peut également être évoqué la situation où le responsable de traitement lui-même n'a pas défini correctement les finalités afin d'exploiter les données massives.

529. Limites de l'effectivité de la suppression des données. Ainsi, au regard du phénomène des données massives, le principe du droit à l'effacement connaît ses propres limites. Lorsque le responsable de traitement a utilisé des modèles d'apprentissage automatique avec des réseaux neuronaux, il devient presque impossible pour ce responsable de supprimer les données ayant enrichi ce modèle. D'une part, il sera extrêmement complexe pour le responsable de traitement

[1453] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, article 17 droit à l'effacement : « 1. La personne concernée a le droit d'obtenir du responsable du traitement l'effacement, dans les meilleurs délais, de données à caractère personnel la concernant et le responsable du traitement a l'obligation d'effacer ces données à caractère personnel dans les meilleurs délais, lorsque l'un des motifs suivants s'applique :
a) les données à caractère personnel ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées d'une autre manière ;
b) la personne concernée retire le consentement sur lequel est fondé le traitement, conformément à l'article 6, paragraphe 1, point a), ou à l'article 9, paragraphe 2, point a), et il n'existe pas d'autre fondement juridique au traitement ;
c) la personne concernée s'oppose au traitement en vertu de l'article 21, paragraphe 1, et il n'existe pas de motif légitime impérieux pour le traitement, ou la personne concernée s'oppose au traitement en vertu de l'article 21, paragraphe 2 ;
d) les données à caractère personnel ont fait l'objet d'un traitement illicite ;
e) les données à caractère personnel doivent être effacées pour respecter une obligation légale qui est prévue par le droit de l'Union ou par le droit de l'État membre auquel le responsable du traitement est soumis ;
f) les données à caractère personnel ont été collectées dans le cadre de l'offre de services de la société de l'information visée à l'article 8, paragraphe 1. ».

d'identifier les données à caractère personnel à supprimer au sein de ces données massives. D'autre part, la suppression pourrait avoir un coût très onéreux pour le responsable de traitement[1454].

530. Responsabilité des responsables de traitements. Une autre limite à propos de l'effectivité du droit à l'effacement doit être soulignée : lorsque la personne concernée effectue la démarche de supprimer certaines de ses données, peut-on être réellement certain de cette suppression par le responsable de traitement. À ce sujet, dès 2011, Monsieur Schrems avait dénoncé les pratiques de la plateforme Facebook consistant à supprimer les données uniquement du côté de l'utilisateur. Le plaignant avait en effet constaté que les informations qu'il avait effacées restaient stockées sur les serveurs de Facebook, notamment des messages privés. Cette pratique a été confirmée par un jugement du Tribunal de Grande Instance (TGI) de Paris le 9 avril 2019 rappelant à la plateforme qu'il est interdit de conserver indéfiniment les données de ses utilisateurs, même après la suppression de leur compte[1455].

Il est légitime de se questionner sur l'effectivité des demandes d'effacement des utilisateurs. Il sera difficile de prouver que les géants du numérique ont réellement supprimé les données de leurs systèmes d'information. En réalité, seuls les acteurs concernés sont en mesure de savoir s'ils ont réellement supprimé les données. L'incertitude des utilisateurs sur la mise en œuvre effective de leurs droits entraîne des risques pour la protection des individus.

[1454] Vergnolle Suzanne, *op. cit.*, p. 311.

[1455] Décision n° 14/07298. La clause litigieuse précisait « Lorsque vous supprimez votre contenu de propriété intellectuelle, ce contenu est supprimé d'une manière similaire au vidage de corbeille sur un ordinateur. Cependant, vous comprenez que les contenus supprimés peuvent persister dans des copies de sauvegarde pendant un certain temps (mais qu'ils ne sont pas disponibles). ». Or, pour l'association UFC-QUE CHOISIR, la clause n°2.2 est illicite étant donné qu'elle n'offre aucune précision sur les modalités de suppression ou sur la durée de conservation des données dans les copies de sauvegarde de la société Facebook. De surcroît, l'association soutenait également que la clause était illicite au regard de l'article 6 de la Loi Informatique et Libertés et de l'article 6 de la directive de 95/46/CE, de l'article 36 de la Loi Informatique et Libertés, lesquels prévoient que la conservation des données sous une forme permettant l'identification des personnes concernées ne peut excéder la durée nécessaire aux finalités pour lesquelles elles sont collectées et traitées et qu'elles ne peuvent être conservées au-delà de cette durée qu'en vue d'être traitées à des fins historiques, statistiques ou scientifique.

II. Les risques de l'inadéquation des principes de protection

531. Tempéraments. Toutes ces limites comportent des risques pour l'effectivité de la protection des personnes concernées. Toutefois, le règlement européen tente de protéger les utilisateurs contre certaines pratiques des acteurs du numérique : il s'agit de protéger les individus lorsqu'ils font l'objet de décisions automatisées (A) et d'encadrer la transmission des données à des tiers (B).

A) Les effets néfastes des décisions automatisées pour les individus

532. Inintelligibilité des algorithmes. L'usage des décisions automatisées est encadré afin de protéger les individus contre l'absence d'appréciation humaine. En réalité, l'encadrement est à nouveau limité au regard de l'opacité des algorithmes d'apprentissage automatique (1). Par conséquent, cela entraîne *de facto* des risques pour les individus (2).

1. L'opacité des algorithmes d'apprentissage automatique

533. L'encadrement des décisions automatisées. Une décision automatisée est une décision « prise à l'égard d'une personne, par le biais d'algorithmes appliqués à ses données personnelles, sans qu'aucun être humain n'intervienne dans le processus[1456] ». Afin de protéger les personnes contre l'absence d'appréciation humaine dans la prise de décision, le Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données prévoit des règles restrictives. En effet, le règlement encadre l'usage des décisions entièrement automatisées et du profilage lorsque ces techniques produisent des effets juridiques ou significatifs pour les personnes. Il peut s'agir d'effets sur la liberté d'aller

[1456] Commission nationale de l'informatique et des libertés, définition décision entièrement automatisée : « Il s'agit d'une décision prise à l'égard d'une personne, par le biais d'algorithmes appliqués à ses données personnelles, sans qu'aucun être humain n'intervienne dans le processus. Les décisions automatisées peuvent intervenir dans de nombreux domaines d'activité (finance, fiscalité, marketing, etc.) et produire des effets juridiques ou des effets significatifs pour les personnes concernées. Par exemple, une décision de refus de crédit peut avoir pour seul fondement l'utilisation d'un algorithme qui applique automatiquement certains critères à la situation financière du demandeur, sans aucune intervention humaine. » ; Rochfeld Judith « L'encadrement des décisions prises par algorithme », Dalloz IP/IT, 2018, p. 474.

et venir, l'accès à certains droits sociaux, à un emploi, un crédit ou encore aboutir à des formes de discrimination[1457].

Le principe est alors le suivant : les personnes ont le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage[1458]. En revanche, le principe ne s'applique pas lorsque la décision est nécessaire à la conclusion ou à l'exécution du contrat ou lorsque la décision est fondée sur son consentement explicite[1459]. Au regard des limites de l'effectivité du consentement, l'exception peut s'avérer dangereuse pour la protection des individus[1460]. En effet, lorsque la personne n'a pas réellement la capacité d'évaluer les conséquences d'une décision entièrement automatisée, elle aura tendance à consentir de manière automatique. L'absence de conscience de l'individu limite la portée du consentement et permet aux sociétés de contourner le principe d'interdiction afin de faire usage des décisions automatisées ou du profilage. L'exception du consentement explicite se retourne finalement contre les individus et bénéficie aux acteurs du numérique.

534. Limites du principe de transparence. Afin d'éclairer les individus sur les décisions automatisées ou le profilage, le responsable de traitement est soumis à une obligation de transparence : le responsable de traitement a l'obligation d'informer de « l'existence d'une prise de décision automatisée, y compris un profilage, des informations utiles concernant la logique sous-jacente, ainsi que l'importance et les conséquences prévues de ce traitement[1461] » lorsque l'intéressé en fait la demande. En pratique, il s'agit de sociétés privées qui peuvent invoquer le secret des affaires ou la protection par la propriété intellectuelle afin de contourner leur

[1457] Basdevant Adrien, « La discrimination algorithmique », *in* G'Sell Florence (dir.), *Le Big Data et le Droit*, éd. Dalloz, 2020, p. 243.

[1458] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, article 22 : « La personne concernée a le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire. » ; Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, article 47.

[1459] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, article 22.2.

[1460] Martial-Braz Nathalie, « L'abus de textes peut-il nuire à l'efficacité du droit ? », Dalloz IP/IT, 459, 2018 : « Le fait qu'aucune décision "ne peut être prise sauf exception", n'a pas la même force que la reconnaissance d'un droit subjectif à ne pas faire l'objet de décision prise sur le fondement d'un profilage. ».

[1461] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, article 13 paragraphe 2) et 14 paragraphe 2) g).

obligation légale de transparence[1462]. L'invocation des secrets protégés par la loi par des sociétés privées constitue une autre limite à l'effectivité de la protection des personnes[1463]. De surcroît, lors de l'utilisation de systèmes de *deep learning*, la transparence du fonctionnement des algorithmes est confrontée à la problématique de la « boîte noire ».

535. La problématique de la « boîte noire ». Le principe de transparence est limité en raison de la nature des algorithmes d'apprentissage automatique puisque ces « objets techniques s'expriment dans un espace qui leur est propre, et qui n'a pas fonction à être humainement compréhensible[1464] ». En effet, la logique des algorithmes d'apprentissage déductifs peut être expliquée par le responsable de traitement puisqu'il a déterminé les règles *ex ante*. En revanche, la logique des algorithmes « inductifs », c'est-à-dire non supervisés, est difficilement interprétable. En réalité, il sera presque impossible pour le responsable de traitement de comprendre le procédé technique ayant abouti à la décision puisque l'algorithme va produire un ensemble de règles dans une forme qui n'est pas accessible à l'humain[1465]. Pour d'aucuns il s'agit de véritables « boîtes noires »[1466] puisque l'idée étant que l'on sait ce qui « entre » d'un côté, on constate ce qui « sort » de l'autre côté, mais on ne sait pas ce qui se passe entre les deux[1467]. Les principes de protection tels que le principe de transparence ou encore le droit d'accès se heurtent donc à la technique : les réseaux de neurones utilisés ne sont pas

---

[1462] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, considérant 63 ; Latil Arnaud, *Le droit du numérique : une approche par les risques,* éd. Dalloz, 2023, p. 47 ; Poullet Yves, *op. cit*., p. 117.

[1463] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, article 47.1 : « Des cas mentionnés aux a et c du 2 de l'article 22 du règlement (UE) 2016/679 du 27 avril 2016, sous les réserves mentionnées au 3 du même article 22 et à condition que les règles définissant le traitement ainsi que les principales caractéristiques de sa mise en œuvre soient communiquées, à l'exception des secrets protégés par la loi, par le responsable de traitement à l'intéressé s'il en fait la demande. ».

[1464] Deltorn Jean-Marc, « Le droit des données personnelles face à l'opacité des algorithmes prédictifs : les limites du principe de transparence », *in* Netter Emmanuel (dir.), *Regard sur le nouveau droit des données personnelles*, éd. Centre de droit privé et de sciences, 2019, p. 153.

[1465] Netter Emmanuel, « La part de l'Homme et celle de la machine dans les « décisions automatisées ». Propositions pour une réécriture de l'article 22 du RGPD », *in* Barbé Vanessa (dir.), *Vers un droit de l'algorithme*, éd. Mare et Martin, 2022.

[1466] Boizard Maryline, « Données à caractère personnel - Le consentement à l'exploitation des données à caractère personnel : une douce illusion ? », CCE, 2016 ; Deltorn Jean-Marc, « Le droit des données personnelles face à l'opacité des algorithmes prédictifs : les limites du principe de transparence », *op. cit.*, p. 195 ; Vergnolle Suzanne, *op. cit.*, p. 459 ; Latil Arnaud, *Le droit du numérique : une approche par les risques*, *op. cit*., p. 44 ; v. à ce sujet : Pascual Frank, *Black box society. Les algorithmes secrets qui contrôlent l'économie et l'information*, éd. FYP, 2015 ; Cardon Dominique, *À quoi rêvent les algorithmes : nos vies à l'heure des big data*, éd. Seuil, 2015, p. 13.

[1467] Rouvroy Antoinette, « La robotisation de la vie ou la tentation de l'inséparation », *op. cit.*, p. 28.

interprétables par l'humain[1468]. Il existe pourtant un principe élémentaire : « si vous n'êtes pas capable d'expliquer aux individus ce que vous faites avec leurs données, alors vous devriez arrêter[1469] ». L'usage d'algorithmes inintelligibles par des sociétés privées entraîne inévitablement des risques pour les utilisateurs.

2. Les risques de l'utilisation des algorithmes

536. Gouvernementalité algorithmique. L'opacité des algorithmes d'apprentissage automatique a pour conséquence une manipulation des individus. L'utilisation de systèmes d'intelligence artificielle permet une certaine « gouvernementalité algorithmique[1470] ». En effet, les algorithmes sont de « simples » constructions mathématiques, il n'existe pas de morale des algorithmes. Pour d'aucuns, il s'agit simplement de « perroquets stochastiques » ou encore de « perroquets probabilistes[1471] ». Néanmoins, l'usage des algorithmes d'apprentissage automatique peut avoir des impacts réels sur les individus. Au regard du principe de gouvernementalité algorithmique, Antoinette Rouvroy précise que dans le domaine du crédit

[1468] Deltorn Jean-Marc, *op. cit*., p.177 : « Ni la personne ayant conçu l'algorithme, ni l'informaticien l'ayant traduit en code informatique, ni le responsable des bases de données ou de la phase d'apprentissage ne sont à même de prédire les caractéristiques précises du modèle qui en est déduit. L'enchaînement déterministe permettant d'arriver à une prédiction échappera à toute traduction : dans le cas des neurones artificiels, les données en entrées seront séquentiellement pondérées, croisées, transformées. À chaque couche de l'architecture, ce brassage non-linéaire produira de nouvelles grandeurs qui subiront à leur tour, à la couche suivante, un nouveau mélange. Alors même que la richesse prédictive des modèles est le fruit de ce mécanisme, déterministe, de croisement, la variété combinatoire qu'il exprime ne pourra se réduire à une interprétation "concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples" ».

[1469] Netter Emmanuel, « Sanction à 50 millions d'euros : au-delà de Google, la CNIL s'attaque aux politiques de confidentialité obscures et aux consentements creux », Dalloz IP/IT, 2019, p. 165.

[1470] Rouvroy Antoinette et Berns Thomas, « Gouvernementalité algorithmique et perspectives d'émancipation. Le disparate comme condition d'individuation par la relation ? », Réseaux, La Découverte, 2013, p. 32 : « La gouvernementalité algorithmique ne produit aucune subjectivation, elle contourne et évite les sujets humains réflexifs, elle se nourrit de données infra-individuelles insignifiantes en elles-mêmes, pour façonner des modèles de comportements ou profils supra-individuels sans jamais en appeler au sujet, sans jamais l'appeler à rendre compte par lui-même de ce qu'il est ni de ce qu'il pourrait devenir. ».

[1471] Bender Emily, Gebru Timnit, Shmitchell Shmargaret *et al*., « On the Dangers of Stochastic Parrots : Can Language Models Be Too Big ? », Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency : « Text generated by an LM is not grounded in communicative intent, any model of the world, or any model of the reader's state of mind. It can't have been, because the training data never included sharing thoughts with a listener, nor does the machine have the ability to do that. This can seem counter-intuitive given the increasingly fluent qualities of automatically generated text, but we have to account for the fact that our perception of natural language text, regardless of how it was generated, is mediated by our own linguistic competence and our predisposition to interpret communicative acts as conveying coherent meaning and intent, whether or not they do. ».

hypothécaire ou crédit à la consommation, les applications du *Big Data* évaluent les risques non pas en fonction de l'individu propre mais d'une certaine proportion statistique. Ainsi, l'évaluation du risque de non-remboursement sera évaluée en fonction de la proportion statistique de mauvais payeurs habitant dans le même quartier, ayant les mêmes habitudes de consommation et utilisant les mêmes plateformes. Le risque de non-remboursement serait alors une sorte de « contagion » que l'individu attraperait en fonction des individus qui lui ressemblent et non pas en fonction de ses caractéristiques propres[1472]. Ainsi, les profils créés sont purement statistiques et peuvent contenir des biais[1473].

537. Discrimination algorithmique. La gouvernementalité algorithmique entraînerait une sorte de « déshumanisation »[1474]. Plusieurs affaires ont démontré le risque de discrimination algorithmique par les acteurs du numérique en l'absence d'appréciation humaine[1475]. À titre d'illustration, dans son rapport annuel de 2016, la *Federal Trade Commission* (l'agence fédérale américaine indépendante pour l'application du droit de la consommation et le contrôle des pratiques commerciales anticoncurrentielles) illustre les risques : plusieurs affaires démontrent que l'utilisation d'algorithmes a abouti au refus de droits à des individus sur la base d'individus similaires. Il a été démontré qu'une société de cartes de crédit diminuait le plafond de certains de ses clients à partir de l'analyse effectuée sur d'autres clients fréquentant les mêmes magasins qu'eux et présentant de mauvais historiques de remboursement. Ainsi, le risque de profilage comportemental entraîne des risques importants pour les individus, surtout lorsque les algorithmes sont conçus de manière opaque par des sociétés privées[1476].

1472 *Ibid*., p. 39.

1473 Poullet Yves, *Le RGPD aux défis de l'intelligence artificielle,* éd. Larcier, 2020, p. 46.

1474 De Nebehay Marin, « De l'intérêt d'un débat sur la gouvernementalité algorithmique », sur IDFRights, publié le 27 octobre 2022.

1475 Pons Ronan et Risser Laurent, « Biais et discriminations dans les systèmes d'intelligence artificielle », Dalloz IP/IT, 2022, pp. 75-78.

1476 Basdevant Adrien, « La discrimination algorithmique », *in* G'Sell Florence (dir.), *Le Big Data et le Droit*, éd. Dalloz, 2015, p. 243 : « Le risque du profilage comportemental, que ce soit pour des applications aussi variées que le maintien de la sécurité nationale ou la prévention des mauvais payeurs, peut conduire à l'établissement de listes noires ou encore de discriminations de toute sorte. Les discriminations algorithmiques constituent ainsi l'un des risques majeurs du recours à ces nouveaux artefacts. Tout citoyen s'expose alors au risque d'être dans l'impossibilité de contester les décisions issues de ces algorithmes qui fonctionnent en toute opacité. » ; Bertrand Brunessen, « La gouvernance des données dans la régulation européenne de l'intelligence artificielle », RTD eur. 2022, n° 315.

538. Absence de neutralité algorithmique. En effet, les systèmes d'exploitation des données peuvent aboutir sur des discriminations en raison de l'absence de neutralité des algorithmes[1477]. La Commission nationale de l'informatique et des libertés soulève en ce sens que l'algorithme « incorpore inévitablement les partis pris - que ceux-ci soient sociaux, politiques, éthiques ou moraux - et répond le plus souvent à des finalités qui incluent une dimension commerciale pour son auteur[1478] ». La problématique de l'opacité de ces systèmes réside dans la finalité commerciale des responsables de traitement. Les géants du numérique développent des algorithmes dont l'objectif principal est la maximisation des revenus. Ainsi, lorsque l'algorithme se nourrit des données disponibles de la plateforme, les biais présents seront simplement reproduits. L'absence de transparence des algorithmes de ces acteurs engendre un risque prégnant pour la liberté de choix des utilisateurs. Au regard des pratiques des géants du numérique, « le soupçon porte autant sur l'algorithme lui-même que ceux qui cherchent à le manipuler[1479]» : les concepteurs reproduisent également des préjugés qui vont engendrer des biais[1480].

Les plateformes du numérique transfèrent une partie de leurs données à des entreprises tierces - également privées - afin d'analyser les données à des fins de revente.

B) La transmission obscure des données à caractère personnel à des tiers

539. Opacité des pratiques des sociétés tierces. Les sociétés conservent les données afin de pouvoir agréger les données pour des usages ultérieurs. Afin d'affiner les analyses de profil des utilisateurs, les données sont également vendues à des sociétés spécialisées dans l'analyse de données. Les pratiques de ces sociétés tierces sont opaques (1), d'autant plus que les individus sont généralement inconscients que leurs données à caractère personnel sont transférées à des tiers (2).

[1477] Latil Arnaud, *Le droit du numérique : une approche par les risques*, éd. Dalloz, 2023, p. 25 sur le « mythe de la neutralité technique ».

[1478] Commission nationale de l'informatique et des libertés, Rapport « Comment permettre à l'homme de garder la main ? Les enjeux éthiques des algorithmes et de l'intelligence artificielle », décembre 2017, p. 29.

[1479] Chignard Simon et Benyayer Louis-David, *Datanomics,* éd. FYP, 2015, p. 71.

[1480] Haas Gérard et Astier Stéphane, « Les biais de l'intelligence artificielle : quels enjeux juridiques ? », Dalloz IP/IT, 2019 : « L'intelligence artificielle, du fait de sa conception humaine, pourra reproduire les préjugés de ses concepteurs et engendrer des biais dits "cognitifs". Ces biais sont liés à la manière dont les algorithmes sont rédigés par les programmateurs. Ils représentent une forme de distorsion de la manière dont l'information est traitée par rapport à un comportement rationnel ou à la réalité. ».

1. L'opacité des pratiques des sociétés d'analyse des données

540. Les catégories de tiers autorisés. Lorsque les utilisateurs prennent conscience de la collecte et de l'exploitation de leurs données, ils sont persuadés que leurs données restent dans les systèmes d'information de la plateforme. En réalité, les responsables de traitement peuvent autoriser la communication de ces données à des tiers. Il peut s'agir d'une « personne physique ou morale, une autorité publique, un service ou un organisme autre que la personne concernée, le responsable de traitement, le sous-traitant et les personnes qui, placées sous l'autorité directe du responsable de traitement ou du sous-traitant, sont autorisées à traiter les données à caractère personnel[1481] ».

Il existe donc plusieurs catégories de tiers pouvant recevoir la communication de données : les sous-traitants, les destinataires et les tiers autorisés. Le sous-traitant est la personne qui traite des données pour le compte du responsable de traitement, étant lié au responsable de traitement par un contrat et ne fait que suivre les instructions du responsable de traitement. En principe, il ne peut pas utiliser les données pour son propre compte[1482]. Il existe également certains destinataires qui sont autorisés à recevoir communication des données à caractère personnel. Le destinataire est « toute personne habilitée à recevoir communication de ces données[1483] ». Les tiers autorisés sont, eux, des organismes pouvant accéder aux données grâce à une loi qui les autorise expressément. Il s'agit généralement des autorités publiques ou des auxiliaires de justice, par exemple l'administration fiscale, les huissiers de justice, les administrations de la justice, de la police ou de la gendarmerie. Ainsi, la différence entre les tiers autorisés et les destinataires est la suivante : les tiers autorisés bénéficient d'une habilitation leur permettant de recevoir communication de ces données.

[1481] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, article 4, point 10).

[1482] *Ibid*., article 4, point 8) : « "sous-traitant", la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement ».

[1483] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, article 3-2 : Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, article 4 point 9) : « "destinataire", la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication de données à caractère personnel, qu'il s'agisse ou non d'un tiers. Toutefois, les autorités publiques qui sont susceptibles de recevoir communication de données à caractère personnel dans le cadre d'une mission d'enquête particulière conformément au droit de l'Union ou au droit d'un État membre ne sont pas considérées comme des destinataires ; le traitement de ces données par les autorités publiques en question est conforme aux règles applicables en matière de protection des données en fonction des finalités du traitement. ».

541. L'intérêt des courtiers en données. En pratique, avec l'objectif de libre circulation des données, les règles sont relativement permissives concernant les tiers autorisés et cette souplesse a permis à des entreprises spécialisées en courtage de données de se développer aux frontières de la légalité. Les courtiers en données sont des entreprises qui collectent, agrègent, transforment et revendent les données à des fins marketing. Ils ont pour objectif d'établir des profils de consommateurs qui seront revendus à des entreprises tels que des annonceurs. Les données qu'ils possèdent sur les individus sont très détaillées : il peut s'agir du modèle de voiture de l'individu, son type de logement, s'il souffre de diabète ou d'un cancer, à quelle fréquence il visionne des vidéos, etc[1484]. Ils collectent les données en les achetant auprès d'organismes ou simplement en collectant les traces laissées par les individus. Le marché des données est devenu un marché « multiface » en raison de la diversité des acteurs traitant les mêmes données[1485]. Le marché multiface est possible grâce aux caractéristiques des données qui permettent à plusieurs personnes de traiter les mêmes données, du fait de leur caractère non rival. De surcroît, les données sont difficilement traçables ce qui permet à des tiers de les exploiter de manière opaque[1486].

La problématique morale de ces entreprises est que les données sont généralement récupérées à l'insu des personnes concernées. Il s'agit à nouveau d'une illustration concrète du consentement « vulnérable » - voire « vide » - donné par l'utilisateur inconscient de cette exploitation de ses propres données.

2. L'inconscience des utilisateurs de l'existence des sociétés

542. L'absence d'information des utilisateurs. En pratique, les utilisateurs cochent une case obligatoire permettant à la plateforme de partager les données avec des tiers et l'information concernant l'identité des tiers est généralement noyée dans les politiques de confidentialité. À titre d'illustration, Facebook précise dans ces conditions d'utilisation transférer les données « à nos *data centers*, partenaires, prestataires de services, fournisseurs, et nos systèmes dans le monde entier, y compris en dehors de votre pays de résidence[1487] ». Il n'est en aucun cas précisé

[1484] Chignard Simon et Benyayer Louis-David, *op. cit*., p.26.
[1485] Monnerie Nils, « Les défis de la commercialisation des données après le RGPD : aspects concurrentiels d'un marché en développement », Revue internationale de droit économique, 2018, pp. 431-452.
[1486] Vergnolle Suzanne, *L'effectivité de la protection des personnes par le droit des données à caractère personnel,* éd. Larcier, 2022, p. 359.
[1487] Conditions de service Facebook version juillet 2023.

de quels types de partenaires ou prestataires il s'agit. Au sein de sa politique de confidentialité, il est indiqué que Facebook partage « les informations que nous recueillons dans le monde entier, à la fois en interne dans nos bureaux et nos *data centers*, et en externe avec nos partenaires et d'autres tiers tels que les prestataires de services » afin « de corriger, d'analyser et d'améliorer nos produits ». Les « informations » sur les « autres tiers » restent obscures dans le dessein de laisser l'individu inconscient des transferts de ses données[1488].

Dès 2014, le Conseil d'État avait soulevé l'absence d'information des utilisateurs : « la transmission de données personnelles d'une entité à une autre est porteuse de risques particuliers : dès lors que l'acquéreur des données est une autre entité que celle qui les a initialement collectées auprès de la personne concernée, ses finalités peuvent être différentes. En outre, en dépit des dispositions de l'article 32 de la loi du 6 janvier 1978 sur le droit d'information, la personne concernée n'est que rarement informée de la cession de ses données et ne sait donc plus qui est le responsable de traitement. Le risque s'accroît lorsque les transmissions se succèdent[1489]. ». Lorsque les personnes concernées n'ont pas conscience de la transmission de leurs données à des tiers, cela porte atteinte à l'effectivité de la protection des personnes[1490].

543. Les risques pour les utilisateurs. L'absence d'information des utilisateurs sur le transfert de leurs données est un risque pour l'effectivité de la protection des personnes. En effet, lorsque les personnes ne sont pas conscientes de l'exploitation de leurs données, il n'est pas possible pour elles d'exercer leurs droits. L'activité de ces courtiers de données est un danger pour les libertés des individus puisqu'ils « blanchissent » leurs activités en se drapant derrière le consentement qu'ils ont extorqué à l'internaute à travers l'acceptation de CGU illisibles et jamais lues[1491].

Afin d'illustrer l'inconscience des utilisateurs sur ces pratiques, il convient de rappeler le scandale de l'affaire Cambridge Analytica. L'ensemble des données récoltées par le test de Facebook avaient ensuite été transférées à l'entreprise de courtage de données afin d'être

1488 Vergnolle Suzanne, *op. cit.*
1489 Conseil d'État, « Le numérique et les droits fondamentaux », Rapport public 2014, Paris, la Documentation française, 2014, p.183.
1490 Vergnolle Suzanne, *op. cit*, p.355.
1491 Cardon Dominique, *À quoi rêvent les algorithmes,* éd. Seuil, 2015, p. 37.

analysées et utilisés à des fins marketing ou pire, politique. En effet, l'entreprise avait été embauchée par Donald Trump lors de sa campagne de 2016. Il est alors légitime de penser que les données ont pu être utilisées pour cibler les électeurs en leur adressant des messages politiques personnalisés. En 2022, la société Méta a payé 725 millions de dollars afin de mettre fin au procès lancé en 2018. Il s'agit assurément d'un « aveu implicite » de la société pour avoir laissé l'accès aux données à des tiers non autorisés[1492]. Néanmoins, malgré l'importance du scandale médiatique de cette affaire, la prise de conscience des utilisateurs est négligeable.

[1492] AFP, « Scandale de Cambridge Analytica : Facebook accepte de payer 725 millions de dollars à la justice », Libération, 2022.

544. Conclusion de la section. Le phénomène du *Big Data* représente un défi majeur pour les acteurs du numérique. Grâce aux données récoltées et à la massification des données, les acteurs peuvent exploiter et analyser une quantité de données démesurée. Le recours aux techniques d'intelligence artificielle permet d'anticiper les comportements des utilisateurs afin de pérenniser l'économie de l'attention et par conséquent, de maximiser leurs revenus.

Afin de protéger les individus contre la collecte massive de leurs données, le Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données instaure des principes fondamentaux de minimisation et de finalité. Les géants du numérique sont soumis à ces obligations lorsqu'ils collectent et exploitent les données de leurs utilisateurs.

Néanmoins, la simple étude du phénomène du *Big Data* met à mal les principes protecteurs. Le principe même du phénomène est de collecter et d'analyser un maximum de données sans en connaître la finalité. Les techniques de *machine learning* ou de *deep learning* vont analyser et développer des corrélations par des usages secondaires des données. De surcroît, le *Big Data* implique nécessairement une collecte massive de données, en totale contradiction avec le principe de minimisation. *In fine,* le développement du *Big Data* vide de sa substance les principes fondamentaux du règlement sur la protection des données à caractère personnel. La prise en compte de ces antinomies rend l'effectivité du cadre normatif superficielle.

Par ailleurs, les géants du numérique exploitent les données de manière inintelligible. En pratique, certaines techniques d'intelligence artificielle ne sont plus compréhensibles pour l'humain et constituent de véritables boîtes noires. L'opacité des algorithmes utilisés par les géants du numérique complique les droits des individus sur leurs données à caractère personnel. En effet, l'absence de transparence de ces pratiques empêche les individus d'exercer leurs droits. Il s'agit d'un paradoxe de la pratique au regard de la théorie : les individus ne peuvent pas exercer leurs droits s'ils sont inconscients des dérives de l'exploitation de leurs données. L'inconscience des utilisateurs constitue également une limite à l'effectivité des principes protecteurs. En réalité, cette inconscience est délibérée puisque pour ces sociétés privées, le principe est de collecter le maximum de données et de les conserver le plus longtemps possible, afin de créer toujours plus de valeur.

545. Conclusion chapitre. L'effectivité d'une norme doit être appréciée au regard des effets réels sur les comportements sociaux. Pour être effective, la règle doit être acceptée par son destinataire. Le Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données a renforcé la protection des individus afin de faire face aux dérives des géants du numérique sur la collecte et l'utilisation des données. Pour ce faire, les droits des individus ont été confirmés et les obligations des responsables renforcés. De grands principes - tels que le principe de minimisation et le principe de finalité - doivent alors guider les acteurs concernés. Les principes du règlement européen doivent être acceptés et respectés par les acteurs du numérique afin de rendre le cadre de protection effectif et d'exploiter les données de manière « responsable ».

Pour autant, l'étude de l'application des normes soulève certaines limites de l'effectivité du cadre. En effet, il existe un écart prégnant entre les principes énoncés et la réalité sociale. Le consentement a été promu pour renforcer le contrôle des individus sur leurs données à caractère personnel. En réalité, le consentement nous semble au contraire « vulnérable » au regard de la puissance certaine des géants du numérique. Par ailleurs, l'asymétrie d'information ne permet pas d'éclairer l'individu sur les pratiques de ces acteurs sur ses données à caractère personnel. Ainsi, lorsque l'utilisateur n'est pas conscient de l'utilisation de ses données, il ne peut exercer ses droits. En ce sens, l'effectivité du cadre protecteur pour les individus nous semble considérablement limitée.

En parallèle, ils font en sorte de recueillir un « consentement superficiel » des individus afin de récolter les données à caractère personnel des utilisateurs. Ils peuvent contourner le consentement par l'utilisation d'une base légale moins contraignante afin de traiter les données. Par ailleurs, ils ne cessent de développer des technologies afin de contourner les grands principes tels que le principe de minimisation et le principe de finalité. Ils se retrouvent parfois eux-mêmes dépassés par leurs propres technologies : les algorithmes d'apprentissage automatique deviennent une véritable boîte noire, concept antinomique au principe de transparence.

En réalité, les géants du numérique ont pour principale source de revenus l'exploitation des données de leurs utilisateurs. Ainsi, tant que les données seront leur modèle d'affaires, ils feront en sorte de pouvoir contourner la législation européenne et d'exploiter ses failles dont ils sont

en partie à l'origine. Afin de tempérer les limites de l'effectivité du cadre normatif, les géants du numérique sont contraints de respecter le cadre par l'application des sanctions.

Chapitre 2 :

Les limites de l'effectivité des sanctions

546. Notion d'effectivité. L'effectivité est définie comme le « caractère d'une règle de droit qui est appliquée réellement[1493] ». La notion d'effectivité ne se limite pas au degré de réalisation dans les pratiques[1494]. Le caractère réel de l'application d'une norme s'apprécie par la conformité des comportements par ses destinataires mais également par la sanction prononcée contre ceux qui ne respectent pas la règle[1495]. Afin de construire un cadre normatif dissuasif, le Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données met en place un système de sanctions autour de deux axes : des sanctions administratives sous la supervision de l'autorité de régulation et un régime de responsabilité à l'égard des individus lors de la méconnaissance de ces droits[1496]. Le règlement a considérablement renforcé le montant des amendes afin de construire un cadre véritablement incitatif et adapté à la puissance des acteurs visés.

Ainsi, l'augmentation des sanctions et l'amélioration des procédures de contrôle constituent des impératifs pour l'effectivité du cadre normatif. En réalité, la mise en œuvre du cadre répressif s'avère complexe pour les individus (**Section 1**) et d'application inégale par les autorités de contrôle (**Section 2**).

[1493] Cornu Gérard, *Vocabulaire juridique*, éd. PUF, p. 339.
[1494] Rocher Guy, « L'effectivité du droit », *in* Lajoie André, Janda Richard et Rocher Guy (dir.), *Théories et émergence du droit : pluralisme, surdétermination et effectivité*, éd. Bruylant, 1998, p. 135.
[1495] Leroy Yann, « La notion d'effectivité du droit », Droit et société, 2011, pp. 715-732.
[1496] Sauron Jean-Luc et Quéméner Myriam, « Le régime de sanction du RGPD : quand la complétude l'emporte sur la cohérence », Dalloz IP/IT, 2018, p. 23.

Section 1 : La complexité du régime répressif pour les personnes concernées

547. Diversité des acteurs et des recours. Afin de s'adapter au caractère transversal des données, le droit a évolué en prenant en compte une diversité d'acteurs susceptibles d'être sanctionnés ainsi qu'un certain nombre de recours pour les personnes concernées. La diversité des acteurs et des recours permet *a priori* de renforcer l'effectivité du régime répressif. En réalité, cette diversité complexifie la mise en œuvre de ce cadre (I). Par ailleurs, l'univers numérique entraîne de réelles difficultés en matière probatoire (II).

I. La complexe mise en œuvre du régime répressif

548. Complexité du cadre. Plusieurs acteurs vont pouvoir garantir la mise en œuvre du cadre répressif. Le règlement instaure un nouveau modèle de gouvernance impliquant des acteurs hétéroclites au niveau national et européen (A). La multiplicité des acteurs entraîne une diversité des recours permettant une répartition entre l'ordre administratif et l'ordre judiciaire (B).

A) La multiplicité excessive des acteurs

549. Identification des acteurs. Les acteurs de la mise en œuvre du cadre répressif peuvent être des acteurs spécialisés en droit de la protection des données à caractère personnel (1) ou des acteurs de droit commun (2).

1. Les acteurs spécialisés

550. La Commission nationale de l'informatique et des libertés. Afin de rendre effective la mise en œuvre du cadre normatif, le règlement européen réaffirme la mise en place d'une autorité publique indépendante chargée de surveiller l'application du règlement[1497]. La Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés prévoit que la

[1497] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, chapitre IV « Autorités de contrôle indépendantes », article 51 : « 1. Chaque État membre prévoit qu'une ou plusieurs autorités publiques indépendantes sont chargées de surveiller l'application du présent règlement, afin de protéger les libertés et droits fondamentaux des personnes physiques à l'égard du traitement et de faciliter le libre flux des données à caractère personnel au sein de l'Union (ci-après dénommée "autorité de contrôle"). 2. Chaque autorité de contrôle contribue à l'application cohérente du présent règlement dans l'ensemble de l'Union. ».

Commission nationale de l'informatique et des libertés est l'autorité de contrôle nationale de l'application du règlement européen[1498]. L'existence de la Commission nationale de l'informatique et des libertés permet de recourir à un organe spécialisé dans la matière qu'il régule[1499].

551. Pouvoirs de sanction. Pour rendre effectif le cadre normatif, il était indispensable de renforcer les pouvoirs de l'autorité de régulation afin de pouvoir réellement contrôler et sanctionner si nécessaire les acteurs concernés et surtout, d'équilibrer les pouvoirs[1500]. En ce sens, la présidente de la Commission nationale de l'informatique et des libertés considère que le renforcement des pouvoirs de l'autorité de contrôle illustre une « nouvelle ère dans la régulation[1501] ». Désormais, la Commission nationale de l'informatique et des libertés - ainsi que ses homologues - disposent de pouvoirs d'enquête, de mesures correctrices et de suspension[1502]. Les différents pouvoirs de la Commission nationale de l'informatique et des libertés sont nombreux mais dont les contours exacts sont encore assez flous[1503]. Le pouvoir d'enquête se traduit par la possibilité d'avoir accès à tous les locaux ainsi qu'à toutes les données (sauf secret-défense ou secret professionnel). Concernant le pouvoir de prendre des mesures correctrices, il s'agit de toutes mesures de mise en conformité du traitement ou des mesures punitives. Pour finir, les pouvoirs de suspensions permettent de prendre des « mesures de sauvegarde » lorsque l'autorité de contrôle estime que le transfert de données dans un pays tiers ne respecte pas les

[1498] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, article 8 : « I. La Commission nationale de l'informatique et des libertés est une autorité administrative indépendante. Elle est l'autorité de contrôle nationale au sens et pour l'application du règlement (UE) 2016/679 du 27 avril 2016. ».
[1499] Favro Karine, « La CNIL, une autorité à "l'âge de la maturité" », Dalloz IP/IT, 2018, p. 464 : « Le terme de régulation n'apparaît pas dans la loi mais les principes qui gouvernent son action ne trompent pas ; le contrôle opéré par la CNIL sur les exigences tenant à la finalité du traitement, à l'accès à l'information et à la proportionnalité relèvent en eux-mêmes de la régulation et concourent à l'équilibre interne du système, à savoir la symétrie d'informations entre responsables de traitement et utilisateurs. Son rôle d'expert, renforcé à l'occasion de la loi du 20 juin 2018(3), contribue à asseoir la régulation. ».
[1500] Degrave Elise, « Des pouvoirs renforcés », *in* Terwagne Cécile de, Rosier Karen, Poullet Yves *et al.* (dir.), *Le règlement général sur la protection des données (RGPD/GDPR)*, éd. Larcier, 2018, p. 606.
[1501] Audition de Mme Isabelle Falque-Pierrotin, Présidente de la Commission nationale de l'informatique et des libertés (CNIL), reprise dans le rapport d'information n°4544 : « [le règlement européen] inaugure une nouvelle ère dans la régulation puisqu'il consacre un changement de paradigme : il s'agit d'alléger considérablement ce que nous appelons les formalités préalables - les déclarations et autorisations - au profit d'une démarche de responsabilisation des acteurs et aussi d'un renforcement des droits des individus ».
[1502] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, article 26.
[1503] Netter Emmanuel, « Le choix de la sanction en droit des données à caractère personnel », CCE, n° 3, mars 2024, p. 3.

garanties prévues par le règlement. Les différents pouvoirs seront affinés avec l'expérience et le temps.

552. Autorité de supervision. Désormais, la Commission nationale de l'informatique et des libertés devient une véritable autorité de « supervision[1504] » : l'autorité de contrôle peut contrôler les organismes et surtout, en cas de manquements constatés, elle peut établir des sanctions. Lors de l'issue d'un contrôle ou de plaintes, en cas de non-respect du règlement ou de la Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, la Commission nationale de l'informatique et des libertés peut engager une procédure de sanction. Il existe deux types de procédure : une procédure ordinaire ou une procédure simplifiée. La procédure de sanction ordinaire implique une formation restreinte de l'autorité de régulation composée de 5 membres et d'un président distinct du président de la CNIL. La formation restreinte analyse le ou les manquements au règlement ou à la loi et décide soit de prononcer un rappel à l'ordre ; d'enjoindre de mettre le traitement en conformité, y compris sous astreinte ; de limiter temporairement ou définitivement un traitement ; suspendre les flux de données ou d'ordonner de satisfaire aux demandes d'exercice des droits des personnes, y compris sous astreinte ou encore prononcer une sanction administrative. La procédure de sanction simplifiée est une procédure en cas de manquement de faible gravité. Le président de la formation restreinte pourra statuer. Dans ce cas, seules certaines mesures sont envisageables telles que : un rappel à l'ordre, enjoindre de mettre en conformité le traitement, ou une sanction administrative d'un montant maximum de 20 000 euros. Contrairement à la procédure de sanction ordinaire, la sanction simplifiée ne pourra jamais être rendue publique. La Commission nationale de l'informatique et des libertés doit cependant disposer des moyens adaptés afin de mener les investigations nécessaires[1505].

553. Comité européen à la protection des données (CEPD). À l'échelle européenne, le Comité européen à la protection des données veille à l'application du règlement dans tous les pays membres de l'Union européenne. Le comité succède à l'ancien groupe de l'article 29, dit « G29 »[1506]. Le CEPD est composé de l'ensemble des chefs des autorités de contrôle de chaque

[1504] Favro Karine, *op. cit*., p. 464.

[1505] Netter Emmanuel, « L'instauration d'une procédure simplifiée de sanction au profit de la CNIL », RTD com. 2022, p. 308 : « Il n'y a alors aucune véritable difficulté juridique. Dans de tels cas, le goulet d'étranglement ne se situera désormais plus au niveau de la formation restreinte, à présent apte à rendre des décisions en masse, mais plutôt au niveau des agents. Même dans des hypothèses élémentaires, instruire des plaintes requiert du personnel. ».

[1506] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, articles 68 à 76.

État membre et du contrôleur européen de la protection des données. Il a pour mission de garantir l'application cohérente du règlement au niveau européen. Pour cela, il peut publier des lignes directrices, des recommandations et bonnes pratiques ou conseiller la Commission. Surtout, il peut émettre des décisions contraignantes afin de trancher des différends entre les autorités de contrôle. Le Comité dispose donc de la personnalité juridique afin de pouvoir user de son pouvoir juridique contraignant, contrairement au G29[1507]. Au sein de cette nouvelle ère de régulation, le Comité européen à la protection des données constitue la « clef de voûte institutionnelle du dispositif de régulation européen[1508] ». L'objectif principal du comité étant d'assurer une cohérence au sein des États membres de l'Union européenne afin d'éviter le *forum shopping* et assurer une certaine effectivité du droit de la protection des données à caractère personnel[1509].

554. Mécanisme de coopération. En outre, la cohérence au sein des États membres est assurée par le mécanisme de coopération entre les différentes autorités nationales de protection des données à caractère personnel. Principalement, le mécanisme est instauré afin de prendre en compte les traitements transfrontaliers, c'est-à-dire les traitements mis en œuvre dans plusieurs États membres. En effet, ce mécanisme est nécessaire à l'ère du numérique où les traitements peuvent avoir lieu dans un État membre et avoir des effets sur les personnes dans plusieurs États membres ou lorsque des organismes sont implantés dans différents États membres. Afin d'établir un réel mécanisme de coopération entre les différentes autorités, le RGPD prévoit plusieurs mécanismes tels que : le guichet unique, l'assistance mutuelle, les opérations conjointes ou encore l'imposition de sanctions communes[1510]. Le mécanisme du guichet unique permet lors d'un manquement relatif à un traitement transfrontalier de décider ensemble de la

[1507] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, article 68 : « Le comité européen de la protection des données est institué en tant qu'organe de l'Union et possède la personnalité juridique. ».

[1508] Code de la protection des données à caractère personnel, commentaire de la section 3 « Comité européen de la protection des données », 5 éd., 2023, p. 211.

[1509] Botchorichvili Nana, « Le rôle des autorités de protection des données », *in* Bensamoun Alexandra, Bertrand Brunessen et Anca Ailincai Mihaela (dir.), *Le règlement général sur la protection des données*, éd. Mare & Martin, 2020, p. 229.

[1510] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, article 61 : « 1. Les autorités de contrôle se communiquent les informations utiles et se prêtent mutuellement assistance en vue de mettre en œuvre et d'appliquer le présent règlement de façon cohérente, et mettent en place des mesures pour coopérer efficacement. L'assistance mutuelle concerne notamment les demandes d'informations et les mesures de contrôle, telles que les demandes d'autorisation et de consultation préalables, les inspections et les enquêtes. ».

sanction grâce à une autorité chef de file qui devient le seul interlocuteur de l'organisme. Pour ce faire, la Commission européenne a mis à disposition des autorités une plateforme nommée IMI (*International Market Information System*). La plateforme permet aux autorités d'échanger des informations, de déterminer l'autorité chef de file et de communiquer leurs positions[1511]. Il s'agit donc d'un lieu d'échanges permettant aux autorités de communiquer facilement entre elles.

555. La Data Protection Commission (DPC). Néanmoins, toutes les autorités nationales ne sont pas sur un pied d'égalité. Selon le règlement européen, l'autorité de contrôle de l'établissement principal, ou de l'établissement unique du responsable de traitement, ou du sous-traitant est compétente pour agir en tant qu'autorité de contrôle chef de file concernant le traitement transfrontalier[1512]. En pratique, les géants du numérique ont majoritairement leur siège social domicilié en Irlande en raison du régime fiscal très favorable pour les sociétés[1513]. À titre d'illustration, les sociétés Facebook, Google, Apple ou Airbnb ont implanté leurs sièges sociaux en Irlande. Ainsi, les potentiels manquements des géants du numérique seront principalement constatés et sanctionnés par l'autorité irlandaise de protection des données désignée comme l'autorité chef de file[1514]. En réalité, les actions de cette autorité de régulation limitent l'effectivité du cadre répressif[1515].

Par-delà les autorités nationales ou européennes, des acteurs de droit commun ont également un rôle à jouer dans la mise en œuvre du régime répressif du règlement européen.

1511 Botchorichvili Nana, *op cit*., p. 230.

1512 Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, article 56.

1513 L'Irlande disposait d'un taux d'imposition des sociétés de 12,5%, soit l'un des taux d'imposition sur les sociétés les plus bas au monde. À titre d'illustration, le Royaume-Uni, lui-même considéré comme un pays favorable dispose d'un taux de 19% et la France d'un taux de 25%. En revanche, depuis 2021, l'Irlande a accepté de relever sa fiscalité et d'imposer un taux minimum effectif des entreprises de 15% face à la pression internationale. Le taux reste toutefois encore très favorable pour les multinationales ; Pouillaude Sibylle, « "Attraper les GAFAM" ou le guichet unique en droit de la protection des données personnelles : fonctionnement, bilan et perspectives », Revue du droit de l'Union européenne, 2023.

1514 Castets-Renard Céline, *Droit du marché unique numérique et intelligence artificielle,* éd. Bruylant, 2020, p. 281.

1515 *Infra.*, n° 601.

2. Les acteurs de droit commun

556. Le juge judiciaire. Au niveau national, les juges judiciaires participent également à cette régulation. Tout d'abord, le règlement européen renforce la compétence du juge civil afin de recevoir des demandes individuelles ou collectives[1516]. Le règlement instaure un mécanisme de responsabilité délictuelle permettant à chaque individu d'obtenir la réparation de son préjudice[1517]. Le juge pénal fait également partie des acteurs disposant d'un rôle renforcé dans le régime répressif des données à caractère personnel. En effet, le Code pénal prévoit une section entière concernant les atteintes aux droits de la personne résultant des fichiers ou des traitements informatiques[1518]. Le volet pénal pourrait servir d'outil de régulation par ses fonctions dissuasives, éducatives, moralisatrices et répressives. En réalité, le contentieux pénal s'avère plutôt rare, voire inexistant, en raison du faible taux de transmission des affaires au parquet par la Commission nationale de l'informatique et des libertés et par l'intérêt relatif des enquêteurs sur ce type d'affaires[1519]. L'absence de contentieux pénal ne rend pas cet outil de régulation crédible[1520]. Il nous semblerait pourtant opportun de se saisir des sanctions pénales afin de rendre plus dissuasif le cadre normatif puisque la sanction se rapporte au comportement du coupable et non au préjudice[1521].

1516 Vergnolle Suzanne, *L'effectivité de la protection des personnes par le droit des données à caractère personnel,* éd. Larcier, 2022, p. 436 : « Pendant longtemps, le juge civil a eu un rôle modeste dans la réalisation du droit des données personnelles. En effet, jusqu'au milieu des années 2010, aucune voie de recours ne lui reconnaissait de compétence particulière. ».

1517 Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, article 82 : « 1. Toute personne ayant subi un dommage matériel ou moral du fait d'une violation du présent règlement a le droit d'obtenir du responsable du traitement ou du sous-traitant réparation du préjudice subi. […] 6. Les actions judiciaires engagées pour exercer le droit à obtenir réparation sont intentées devant les juridictions compétentes en vertu du droit de l'État membre visé à l'article 79, paragraphe 2. ».

1518 Code pénal, articles 226-16 à 226-24 ; Article 226-16 : « 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 prévues par la loi est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende. ».

1519 Vergnolle Suzanne, *op. cit*., p.435 ; De surcroit, dès 1988, le conseiller d'État Braibant estimait déjà que « Le régime répressif français en matière de fichiers informatiques - dont la cohérence avec d'autres dispositions du Code pénal comparables est sujette à caution - se caractérise par une grande sévérité, dont le contraste avec une jurisprudence pusillanime est frappant. », Rapport au Premier ministre sur la transposition en droit français de la directive n°95/46, « Données personnelles et société de l'information », 1998, p. 119.

1520 Frayssinet Jean, « La régulation du respect de la loi Informatique, fichiers et libertés par le droit pénal », Légicom, n° 42, Victoires éditions, 2009.

1521 Rochfled Judith, *Les grandes notions du droit privé*, éd. PUF, 2022, p. 667 ; Martial-Braz Nathalie, « L'articulation des différentes sanctions : les alternatives à la sanction administrative », CCE, n° 3, mars 2024 sur l'utilité de la sanction pénale.

557. Le juge administratif. Le juge administratif est également compétent pour recevoir des demandes individuelles ou collectives contre l'administration. En effet, la Commission nationale de l'informatique et des libertés n'a pas le pouvoir d'imposer des amendes administratives à l'État, ce que le juge administratif pourra compenser[1522]. De surcroît, le Conseil d'État en tant que juge administratif suprême est également compétent pour connaître les recours contre les décisions du tribunal administratif prononcées en dernier ressort, contre les décisions des cours administratives d'appel[1523] ou encore contre les recours pour excès de pouvoir contre les décisions de la Commission nationale de l'informatique et des libertés.

Toutefois, il convient de se demander s'il n'aurait pas été plus pertinent de limiter la compétence des juges à certains juges spécialisés, à l'instar du mécanisme de spécialisation en propriété intellectuelle[1524]. De manière concomitante, il existe donc une diversité de recours contre les différents acteurs.

B) La diversité évolutive des recours

558. Les différents recours. Le règlement européen instaure diverses voies de recours afin de tenter de renforcer l'effectivité du droit pour la protection des données à caractère personnel. Il existe des recours auprès et contre l'autorité de contrôle (1) et des recours contre un responsable de traitement ou un sous-traitant (2).

1. Les recours auprès d'une autorité de contrôle

559. Réclamation auprès d'une autorité de contrôle. Lorsqu'une personne estime que le traitement de ses données à caractère personnel constitue une violation du règlement européen, elle peut introduire une réclamation auprès de l'autorité de contrôle de l'État membre dans

[1522] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, article 20, paragraphe III, 7.
[1523] Code de justice administrative, article L.111-1.
[1524] Code de l'organisation judiciaire, article L211-10 : « Des tribunaux judiciaires spécialement désignés connaissent des actions en matière de propriété littéraire et artistique, de dessins et modèles, de brevets d'invention, de certificats d'utilité, de certificats complémentaires de protection, de topographie de produits semi-conducteurs, d'obtentions végétales, d'indications géographiques et de marques, dans les cas et conditions prévus par le code de la propriété intellectuelle. ».

lequel se trouve sa résidence habituelle, son lieu de travail ou le lieu où la violation aurait été commise[1525]. La possibilité d'introduire une réclamation auprès d'une autorité de contrôle a simplement été confirmée par le règlement puisqu'elle existait déjà dans la 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. Au niveau national, les réclamations seront donc portées devant la Commission nationale de l'informatique et des libertés, de manière individuelle ou de manière collective[1526]. Cette possibilité du recours auprès d'une autorité de contrôle présente l'avantage d'émaner d'un organe spécialisé dans la matière qu'il régule[1527]. L'autorité de régulation procédera à un examen afin de déterminer si les droits de la personne n'ont effectivement pas été respectés, avec davantage de célérité que le pouvoir judiciaire.

560. Recours contre l'autorité de contrôle. Le droit de réclamation auprès de l'autorité de contrôle intervient sans préjudice de tout autre recours administratif ou juridictionnel. Ainsi, l'autorité de contrôle a pour obligation d'informer la personne concernée de l'état d'avancement de sa réclamation et à l'issue, de la possibilité d'un recours juridictionnel. En effet, toute personne physique ou morale a le droit de former un recours juridictionnel effectif contre la décision juridiquement contraignante d'une autorité de contrôle. Ainsi, chaque personne a le droit à un recours juridictionnel contre une décision de l'autorité de contrôle mais également contre l'inertie de celle-ci. L'action est intentée devant les juridictions de l'État membre sur le territoire duquel l'autorité de contrôle est établie[1528]. Le recours contre l'autorité de contrôle permet de garantir une cohérence en cas de manquement de l'autorité de régulation ou d'inertie de cette dernière. Par ailleurs, il existe également les recours contre un responsable de traitement ou un sous-traitant.

1525 Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, article 77.

1526 *Ibid*., article 80 ; Loi n°78-17 du 6 janvier 1978, article 38.

1527 Gérard Loïck, « Les sanctions en cas de non-respect du RGPD : vers une plus grande effectivité de la protection des données à caractère personnel ? », *in* De Terwangne Cécile et Rosier Karen (dir.), *Le Règlement général sur la protection des données (RGPD / GDPR). Analyse approfondie*, éd. Larcier, 2018, p. 642.

1528 Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, article 78.

2. Les recours contre un responsable de traitement ou un sous-traitant

561. Recours juridictionnel effectif contre un responsable de traitement ou un sous-traitant. La personne concernée peut également directement intenter une action contre le responsable de traitement ou le sous-traitant lorsqu'elle estime que ses droits ont été violés lors d'un traitement de ses données à caractère personnel[1529]. L'action sera intentée devant les juridictions de l'État membre dans lequel le responsable de traitement ou le sous-traitant dispose d'un établissement, ou devant les juridictions de l'État membre dans lequel la personne concernée a sa résidence habituelle.

562. Articulation des voies de recours. Le règlement européen prévoit un droit d'exercer de façon concurrente et indépendante les voies de recours précitées. La personne concernée peut exercer les voies de recours prévues devant l'autorité de contrôle et contre la décision de l'autorité de contrôle ainsi qu'un recours contre le responsable de traitement ou le sous-traitant. Le règlement prévoit en effet que le droit de réclamation auprès d'une autorité de contrôle est « sans préjudice de tout autre recours administratif ou juridictionnel » et le droit à un recours juridictionnel contre une autorité de contrôle ou contre un responsable de traitement est « sans préjudice de tout autre recours administratif ou extrajudiciaire ». Ainsi, la Cour de justice de l'Union européenne a précisé que « chacune des voies de recours doit pouvoir être exercée "sans préjudice" des autres » : il n'existe pas de voie prioritaire[1530]. En pratique, le choix de la voie de recours dépendra des intérêts de la personne concernée[1531]. Lorsque la personne souhaite faire cesser les agissements sans obtenir de dommages-intérêts, l'action devant l'autorité de contrôle est adéquate. En revanche, le recours devant un juge permet d'obtenir des dommages-intérêts en réparation du préjudice subi.

563. Recours collectif. Afin de faciliter les recours et de renforcer l'effectivité de la protection, le règlement autorise la représentation des personnes concernées. Les personnes peuvent mandater un organisme, une organisation ou une association à but non lucratif afin de

---

1529 *Ibid*., article 79.

1530 Cour de justice de l'Union européenne, aff. n° C-132/21, Budapesti Elektromos, 12 janvier 2023.

1531 Pailler Ludovic, « La Cour de justice de l'Union européenne, pompier pyromane malgré elle : l'articulation des voies de recours ouvertes à la personne concernée par un traitement de données à caractère personnel », sur Légipresse, 2023, p. 161 ; Saillant Clara, « Les recours prévus par le RGPD peuvent être exercés simultanément et de manière indépendante », Dalloz Actualité, 25 janvier 2023.

les représenter. La personne morale doit être active dans le domaine de la protection des droits et libertés des personnes concernées dans le cadre de la protection des données à caractère personnel[1532]. Au niveau national, le droit avait anticipé l'ouverture des recours collectifs[1533]. En effet, concernant la représentation des personnes, le droit de la consommation prévoyait dès le début des années 1990 une « action en représentation conjointe »[1534]. Désormais, l'article 38 de la Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés a introduit l'action en représentation collective[1535]. Les personnes concernées peuvent donc mandater un organisme afin de les représenter pour obtenir la cessation illicite ou pour obtenir réparation du préjudice subi à la suite d'un manquement. Néanmoins, la rigidité de la procédure d'obtention du mandat réduit la portée de cette action[1536]. L'usage du recours collectif en droit de la consommation était déjà limité, d'aucuns évoquant une action « morte-née[1537] ». En droit de la protection des données à caractère personnel, cette action est également inefficace pour le moment. Par conséquent, le règlement européen a ouvert la possibilité pour les États membres

1532 Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, article 80 paragraphe 1.

1533 Danis-Fatôme Anne, « Quelles actions judiciaires en cas de violation du RGPD ? », CCE, avril 2018.

1534 Loi n° 92-60 du 18 janvier 1992 renforçant la protection des consommateurs, articles 8 à 8-3 : « Lorsque plusieurs consommateurs, personnes physiques, identifiés ont subi des préjudices individuels qui ont été causés par le fait d'un même professionnel, et qui ont une origine commune, toute association agréée et reconnue représentative sur le plan national en application des dispositions de l'article 2 de la présente loi peut, si elle a été mandatée par au moins deux des consommateurs concernés, agir en réparation devant toute juridiction au nom de ces consommateurs. » ; Code de l'environnement, article L.142-3 (version en vigueur depuis le 21 septembre 2000) : « Lorsque plusieurs personnes physiques identifiées ont subi des préjudices individuels qui ont été causés par le fait d'une même personne et qui ont une origine commune, dans les domaines mentionnés à l'article L. 142-2, toute association agréée au titre de l'article L. 141-1 peut, si elle a été mandatée par au moins deux des personnes physiques concernées, agir en réparation devant toute juridiction au nom de celles-ci. ».

1535 Loi n° 78-17 du 6 janvier 1978, article 38 : « Toute personne peut mandater une association ou une organisation mentionnée au IV de l'article 37, une association ou une organisation dont l'objet statutaire est en relation avec la protection des droits et libertés lorsque ceux-ci sont méconnus dans le cadre d'un traitement de données à caractère personnel, ou une association dont cette personne est membre et dont l'objet statutaire implique la défense d'intérêts en relation avec les finalités du traitement litigieux, aux fins d'exercer en son nom les droits prévus aux articles 77 à 79 et 82 du règlement (UE) 2016/679 du 27 avril 2016. Elle peut également les mandater pour agir devant la Commission nationale de l'informatique et des libertés, contre celle-ci devant un juge ou contre le responsable de traitement ou son sous-traitant devant une juridiction lorsqu'est en cause un traitement relevant du titre III de la présente loi. ».

1536 Danis-Fatôme Anne, *op. cit*.

1537 Bore Louis, « L'action en représentation conjointe : class action française ou action mort-née ? », Dalloz, 1995, p. 267 ; À titre d'illustration de la rigidité de cette action : les associations ont l'interdiction de faire usage de « tout appel public par moyen de communication de masse ou par lettre personnalisée », Cour de cassation, 1ère, 26 mai 2011, n° 10-15.676 ; Vergnolle Suzanne, *op. cit*., p. 437 : « le déséquilibre entre l'investissement requis et son résultat n'encourage pas les groupements à privilégier ce type de recours ».

d'introduire une action collective indépendamment de tout mandat[1538]. À l'instar de l'action en représentation conjointe, la loi n°2016-1547 du 18 novembre 2016 avait étendu l'action de groupe créée en 2014 en droit de la consommation à la protection des données à caractère personnel[1539]. L'action de groupe figurait donc déjà à l'article 43ter de la Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Néanmoins, l'action permettait uniquement la cessation du manquement, sans possibilité de réparation des dommages, démontrant la faiblesse de cette action.

564. Élargissement de l'action de groupe. Ainsi, la réforme législative du 20 juin 2018 relative à la protection des données à caractère personnel a élargi cette action de groupe à la réparation des préjudices matériels ou moraux subis. Désormais, l'action de groupe est ouverte aux associations régulièrement déclarées depuis cinq ans ayant dans leur objet statutaire la protection de la vie privée ou la protection des données à caractère personnel ; aux associations de défense des consommateurs représentatives au niveau national lorsque le traitement de données à caractère personnel affecte des consommateurs et aux organisations syndicales de salariés ou de fonctionnaires représentatives lorsque le traitement affecte les intérêts des personnes que les statuts de ces organisations les chargent de défendre[1540]. Les organismes précités peuvent former des recours en réparation devant le juge civil suite à une mise en demeure infructueuse. Le recours en réparation doit respecter trois étapes successives par le juge : il statue sur la responsabilité du défendeur, définit le groupe de personnes susceptibles de bénéficier de l'action de groupe, et pour finir fixe les délais permettant aux victimes d'adhérer au groupe[1541]. Lorsque la procédure est respectée et que les manquements sont constatés, l'organisme devra indemniser chacune des personnes. L'action de groupe permet donc de renforcer la protection des individus en rendant plus accessible les recours devant le juge civil[1542].

[1538] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, article 80 paragraphe 2 : « Les États membres peuvent prévoir que tout organisme, organisation ou association visé au paragraphe 1 du présent article, indépendamment de tout mandat confié par une personne concernée, a, dans l'État membre en question, le droit d'introduire une réclamation auprès de l'autorité de contrôle qui est compétente en vertu de l'article 77, et d'exercer les droits visés aux articles 78 et 79 s'il considère que les droits d'une personne concernée prévus dans le présent règlement ont été violés du fait du traitement. ».

[1539] Loi n°2014-344 du 17 mars 2014, dite « Loi Hamon », articles 1 et 2.

[1540] Loi n° 78-17 du 6 janvier 1978, article 37, IV.

[1541] Loi n° 2016-1547 du 18 novembre 2016, article 66.

[1542] Zolynski Célia, « Les nouveaux contours de l'action de groupe et de l'action collective au lendemain de la loi pour la protection des données : un empowerment renforcé », Dalloz IP/IT, 2018, p. 470.

En réalité, les recours juridictionnels sont peu utilisés par les personnes pour le moment[1543]. L'étude des conditions de fond démontre la complexité du cadre pour les individus concernés.

II. La construction incertaine du régime répressif

565. Adaptation des conditions de responsabilité civile. Afin d'obtenir réparation des atteintes à la protection de leurs données à caractère personnel, les individus peuvent invoquer l'article 82 du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données. Il s'agit des conditions classiques de la responsabilité civile, adaptées à l'univers numérique. En effet, le demandeur doit établir un fait générateur de responsabilité (A), un dommage ainsi qu'un lien de causalité (B).

A) Le fait générateur de responsabilité : une notion simplifiée

566. Fait générateur de responsabilité. Le fait générateur de responsabilité en matière de protection des données à caractère personnel se caractérise par la violation du règlement européen (1). Afin de renforcer l'effectivité de la protection des personnes, le règlement instaure un partage de responsabilité entre le responsable de traitement et le sous-traitant (2).

1. La nature de la responsabilité

567. Une violation du règlement. Le règlement européen renforce les obligations des responsables de traitements et par conséquent, le non-respect des obligations prescrites va déclencher la responsabilité du responsable de traitement. La responsabilité sera caractérisée du fait d'un simple manquement aux obligations. La démonstration d'une faute à proprement parler ne serait pas exigée : il existerait une présomption de responsabilité du seul fait de l'existence d'une violation du règlement[1544]. En effet, le règlement évoque que le fait générateur

[1543] Maisnier-Boché Lorraine, « Le défi de l'amélioration des droits des parties dans le cadre des procédures de contrôle et de sanction », CCE, n° 4, avril 2024.

[1544] Rosier Karen et Delforge Antoine, « Le régime de la responsabilité civile du responsable de traitement et du sous-traitant dans le RGPD », *in* Terwangne Cécile de, Rosier Karen, Poullet Yves *et al*. (dir.), *Le règlement général sur la protection des données (RGPD/GDPR)*, éd. Larcier, pp. 665-698 : « Il est probable que le non-respect de certaines dispositions du règlement n'est pas de nature à justifier la mise en cause de la responsabilité si le traitement lui-même n'est pas en cause également. Ainsi en est-il du non-respect

est « une violation du présent règlement[1545] ». Néanmoins, le considérant 146 restreint le fait générateur en précisant qu'il s'agit du fait « d'un traitement effectué en violation du présent règlement[1546] ». Ainsi, il doit s'agir d'un manquement relatif à un traitement et non tout manquement possible[1547]. Les manquements sont toutefois nombreux et divers : ils peuvent résulter de la méconnaissance des principes applicables à tout traitement des données comme l'absence de base juridique adéquate, le détournement de la finalité du traitement, son illicéité ou encore le non-respect du régime de la sous-traitance[1548].

568. Conditions de droit commun. Afin d'engager la responsabilité du responsable de traitement ou du sous-traitant, les conditions classiques de la responsabilité civile doivent être respectées, c'est à dire une violation du règlement, un dommage matériel ou moral résultant de cette violation et un lien de causalité entre le dommage et la violation. Le 4 mai 2023, la Cour de Justice a eu l'occasion de rappeler que la simple violation du règlement européen ne fonde pas un droit à réparation, les trois conditions étant cumulatives[1549]. Par ailleurs, la Cour précise que l'action en réparation auprès d'une juridiction se distingue de l'action en réparation auprès d'une autorité de contrôle : « l'action en réparation se distingue d'autres voies de recours prévues par le RGPD, notamment celles permettant d'infliger des amendes administratives, pour lesquelles l'existence d'un dommage individuel n'a pas à être démontrée ». La première action implique l'indemnisation d'un préjudice individuel tandis que la seconde action administrative implique une sorte de « punition » pour laquelle un préjudice n'a pas à être démontré.

---

d'exigences destinées à aider le responsable de traitement à se conformer au principe de responsabilité (principe d'"accountability"). Le fait qu'un responsable du traitement ait omis de tenir un registre des activités de traitement, de désigner un délégué à la protection des données ou encore de réaliser une analyse d'impact serait donc des éléments non pertinents pour fonder une demande d'indemnisation si ces seuls éléments n'ont pas de conséquences pour la personne dont les données sont traitées. ».

[1545] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, article 82 : « 1. Toute personne ayant subi un dommage matériel ou moral du fait d'une violation du présent règlement a le droit d'obtenir du responsable du traitement ou du sous-traitant réparation du préjudice subi. ».

[1546] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, considérant 146, paragraphe 1 : « Le responsable du traitement ou le sous-traitant devrait réparer tout dommage qu'une personne peut subir du fait d'un traitement effectué en violation du présent règlement. ».

[1547] Knetsch Jonas, « Les actions civiles en réparation fondées sur une violation du RGPD : Vers un nouveau contentieux de masse ? », La Semaine Juridique Edition Générale, publié le 26 septembre 2022.

[1548] Douville Thibaut, « La responsabilité des responsables du traitement et des sous-traitants à l'égard des personnes concernées : une grande oubliée », RAE, 2021, p. 29.

[1549] Cour de justice de l'Union européenne, aff. C-300/21, Österreichische Post, 4 mai 2023 ; Vandevelde Maya, « La violation du RGPD ne suffit pas à ouvrir droit à réparation : il faut aussi prouver un préjudice », Dalloz, 5 juin 2023.

569. Responsabilité extracontractuelle et contractuelle. En droit de la protection des données à caractère personnel, la responsabilité délictuelle et la responsabilité contractuelle peuvent être invoquées. En effet, lorsqu'un contrat constitue le fondement du traitement litigieux, la responsabilité du responsable de traitement sera de nature contractuelle. En revanche, la responsabilité délictuelle pourra s'appliquer lors de la méconnaissance d'une règle de droit. En pratique, la responsabilité délictuelle sera le plus souvent invoquée lors de la méconnaissance d'une règle invoquée par le règlement européen[1550].

570. Inversion de la charge de la preuve. En droit de la responsabilité civile, la preuve de la faute, du préjudice et du lien de causalité incombe à la victime. Afin de faciliter l'action en responsabilité en droit de la protection des données à caractère personnel, la charge de la preuve serait inversée. Effectivement, l'article 24 du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données dispose que « le responsable de traitement met en œuvre des mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément au présent règlement ». Il s'agit de l'illustration du principe d'*accountability* qui incombe au responsable de traitement et au sous-traitant. L'inversion de la charge de la preuve est cohérente dans la mesure où il sera difficile pour la victime de rapporter la preuve du manquement dans l'univers numérique. De surcroît, lorsque le responsable de traitement a respecté les obligations du règlement, il sera plus aisé pour lui de démontrer sa conformité.

[1550] Danis-Fatôme Anne, « Quelles actions judiciaires en cas de violation du RGPD ? », CCE, avril 2018, note 23 : « Dans l'hypothèse où un contrat unissant la personne concernée et le responsable de traitement constitue le fondement du traitement, les obligations qui incombent à ce dernier pourraient avoir une nature contractuelle et leur violation déboucher sur une responsabilité de cette nature. Il faut cependant rappeler que les obligations contractuelles n'ont pas en principe pour vocation d'imposer des règles de conduites. Les obligations contenues dans le RGPD garderont donc dans ce cas une nature légale et déboucheront donc sur une responsabilité délictuelle. ».

2. Le partage de la responsabilité

571. Responsabilité solidaire. Le responsable de traitement est le principal responsable des obligations lui incombant. En revanche, lorsque le responsable de traitement a effectué des traitements de manière conjointe avec un sous-traitant, ils sont responsables de manière solidaire. L'article 82 du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données prévoit le partage de responsabilité entre les deux acteurs : « lorsque plusieurs responsables du traitement ou sous-traitants ou lorsque, à la fois, un responsable de traitement et un sous-traitant participent au même traitement […] chacun des responsables du traitement ou des sous-traitants est tenu responsable du dommage dans sa totalité afin de garantir à la personne concernée une réparation effective[1551] ». Dans certains cas, le partage de responsabilité nous semble délicat à déterminer.

Afin de tempérer la possible difficulté de détermination du partage, la responsabilité solidaire prévue par le règlement est également en faveur des victimes. En effet, la victime n'a pas forcément la connaissance des rôles attribués à chacun dans le traitement des données à caractère personnel. La responsabilité solidaire permet à la victime d'agir contre l'acteur dont elle a la connaissance, à charge pour lui de réclamer une action récursoire par la suite. Lorsque le responsable de traitement ou le sous-traitant est également responsable, il aura l'obligation de lui verser une somme proportionnelle à sa responsabilité. En revanche, le responsable de traitement ou le sous-traitant peut prouver que le fait ayant provoqué le dommage ne lui est nullement imputable.

572. Exonération de la responsabilité. Dans ce cas, il sera exonéré de sa responsabilité. Pour ce faire, il devra prouver que le dommage ne lui est « nullement imputable ». Le terme « nullement » restreint considérablement les possibilités d'exonération et semble nécessiter un niveau de preuve élevé. Il doit prouver son absence de faute ou que la violation lui est totalement étrangère. Il s'agit de la théorie de l'équivalence des conditions selon laquelle la personne fautive n'est pas considérée comme ayant causé le dommage si « le dommage se serait néanmoins produit tel qu'il s'est réalisé sans cette faute, toutes les autres conditions restant

[1551] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, article 82.4.

identiques »[1552]. Dans l'affaire C 340/21, l'avocat général estime que le fait que la violation du RGPD ait été commise par un tiers ne constitue pas en soi une cause d'exonération de responsabilité pour le responsable de traitement. Afin d'être exonéré, il devra démontrer, avec un niveau de preuve élevé, que le dommage ne lui ait nullement imputable. En cas de traitement illicite de données, le régime de responsabilité devient un régime de responsabilité aggravée pour faute présumée[1553].

Le partage de responsabilité est simplifié afin de faciliter la caractérisation du fait générateur, ce qui semble être indispensable pour rendre possible les recours des victimes. Ainsi, sauf exonération de la responsabilité, le responsable de traitement devra réparer le dommage qui lui est imputable lorsque les conditions cumulatives sont réunies.

B) La réparation du dommage : une notion en construction

573. Réparation effective. Le Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données impose une réparation effective du dommage matériel ou moral. Néanmoins, l'évaluation du dommage en matière de protection des données à caractère personnel s'avère délicate (1). De surcroît, l'environnement technique des données complexifie l'apport de preuves tangibles par la victime (2).

1. La difficulté d'évaluation du dommage

574. Existence d'un « dommage matériel ou moral ». Afin de mettre en œuvre la responsabilité du responsable de traitement ou du sous-traitant, la victime doit apporter la preuve d'un dommage matériel ou moral[1554]. La notion de dommage n'étant pas définie précisément par le règlement européen, le considérant 146 du règlement précise que cette notion « devrait être interprétée au sens large, à la lumière de la jurisprudence de la Cour de justice,

[1552] Rosier Karen, Delforge Antoine, « Le régime de la responsabilité civile du responsable de traitement et du sous-traitant dans le RGPD », *op. cit.*, p. 689.
[1553] Cour de justice de l'Union européenne, communiqué de presse n°67/23, Luxembourg, le 27 avril 2023, conclusions de l'avocat général Pitruzzella dans l'affaire C-340/21.
[1554] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, article 82, 1 : « Toute personne ayant subi un dommage matériel ou moral du fait d'une violation du présent règlement a le droit d'obtenir du responsable du traitement ou du sous-traitant réparation du préjudice subi. ».

d'une manière qui tienne pleinement compte des objectifs du présent règlement ». Ainsi, tout dommage devrait être réparé, quelle que soit sa nature, au regard des objectifs du règlement. Afin de préciser et d'unifier la notion de dommage, le considérant 85 du règlement européen établit une liste non exhaustive de situations concrètes telles qu' « une perte de contrôle sur leurs données à caractère personnel ou la limitation de leurs droits, une discrimination, un vol ou une usurpation d'identité, une perte financière, un renversement non autorisé de la procédure de pseudonymisation, une atteinte à la réputation, une perte de confidentialité de données à caractère personnel protégées par le secret professionnel ou tout autre dommage économique ou social important ».

Il s'agit d'identifier les risques qui peuvent entraîner potentiellement des « dommages physiques, matériels ou un préjudice moral »[1555]. Le dommage matériel peut être défini comme le dommage portant atteinte au patrimoine d'une personne[1556]. La notion de dommage matériel renvoie habituellement aux intérêts économiques : il peut s'agir d'une perte subie ou un gain manqué. En matière de protection des données à caractère personnel, le gain manqué peut être l'impossibilité de contracter un emprunt à la suite d'une divulgation de données à caractère personnel à un établissement de crédit ou à une compagnie d'assurance[1557].

575. La notion du « dommage moral ». En revanche, le dommage moral a pendant longtemps été une notion controversée[1558] : « le préjudice moral ressemble actuellement à une mosaïque dont les fragments continuent de se multiplier au gré de l'imagination des

[1555] De Terwangne Cécile et Rosier Karen, « Une obligation de sécurité axée autour des risques pour les personnes physiques », *in* De Terwangne Cécile et Rosier Karen *et al.* (dir.), *Le règlement sur la protection des données, Analyse approfondie*, éd. Larcier, 2018, p. 189.

[1556] Cornu Gérard, *Vocabulaire juridique*, éd. PUF, 2020, p. 365 ; Poullet Yves, *La sécurité informatique, entre technique et droit, éd. Centre de recherches informatique et droit*, 1998, p. 20.

[1557] Danis-Fatôme Anne, *op. cit*.

[1558] L'indemnisation du dommage moral est déjà controversée en droit de la responsabilité civile. La prise en compte de ce dommage a pendant longtemps divisé la doctrine en raison de son caractère trop subjectif. Néanmoins, la jurisprudence a rapidement introduit l'indemnisation du dommage moral ; Terré François, Simler Philippe, Lequette Yves, Chénedé François, *Droit civil, Les obligations,* éd. Dalloz, p. 1020 : « Lorsque le préjudice subi cesse d'être corporel et revêt un caractère extrapatrimonial, sa réparation peut susciter des objections, soit d'une manière générale, parce qu'il est alors singulièrement difficile d'aménager une réparation adéquate, soit de manière plus particulière parce qu'il s'agit d'une douleur morale, car il peut être choquant d'aller en quelque sorte monnayer ses larmes devant les tribunaux (Ripert Georges, Le prix de la douleur, 1948) » ; Molfessis Nicolas, « La psychologisation du dommage », *in* Molfessis Nicolas, *Quel avenir pour la responsabilité civile ?,* éd. Dalloz, 2015.

plaideurs »[1559]. Le dommage moral est un dommage portant atteinte à la considération, à l'honneur, à l'affection ou à un élément de la joie de vivre d'une personne[1560]. Il existe plusieurs types de dommage moral tels que le préjudice d'angoisse ou encore le préjudice lié à la douleur[1561]. La difficulté de la prise en compte du dommage moral est inéluctablement son évaluation puisqu'il s'agit de compenser une souffrance morale avec une évaluation pécuniaire.

Dès lors, la notion de dommage moral en matière de protection des données à caractère personnel est également une notion hésitante[1562]. En effet, les violations du règlement européen s'apparentent généralement à une atteinte aux droits de la personnalité. Il convient en effet de protéger des intérêts individuels afin de réparer les préjudices extrapatrimoniaux. En matière de dommage moral, il peut s'agir d'un simple sentiment d'inconfort à une atteinte majeure de la vie privée. Dans certains cas de traitements illicites ou de divulgations de données, le dommage moral peut être minime telle une avalanche de spams ou des sollicitations indésirables[1563]. Au contraire, il peut y avoir de graves conséquences telle qu'une usurpation d'identité. En fonction de l'atteinte - et de ses conséquences - le dommage moral sera évalué selon les circonstances. Dès lors, la prise en compte du dommage moral est importante en droit de la protection des données à caractère personnel et est encore une notion en construction dont les contours seront déterminés par la jurisprudence.

1559 Knetsch Jonas, « La désintégration du préjudice moral », Recueil Dalloz, 2015, 443 : « Le préjudice moral en ressort profondément désintégré, car divisé en autant de morceaux que de façons dont peut s'exprimer la souffrance humaine. ».

1560 Cornu Gérard, *op. cit*.

1561 Rochfeld Judith, *Les grandes notions du droit privé*, éd. PUF, 2022, p. 622.

1562 De Terwangne Cécile et Rosier Karen, *op. cit*., p. 686 : « Sous l'empire de la Directive, la prise en compte du dommage moral avait déjà été consacrée en jurisprudence. Tel était notamment le cas dans un célèbre arrêt (Court of Appeal (Civil Division), Google Inc v Vidal-Hall & Ors [2015] EWCA Civ 311 (27 March 2015) au Royaume-Uni aux termes duquel une cour d'appel avait condamné Google pour violation à la législation anglaise relative à la protection des données et à la réparation des dommages moraux subis suite à cette violation. Cette affaire demeure particulièrement intéressante à rappeler puisque la cour d'appel avait notamment fait usage des dispositions de la Charte des droits fondamentaux de l'Union européenne (art. 8 et 47 combinés) pour justifier que, au nom du droit à avoir un recours effectif, la notion de dommage réparable en vertu de l'article 23 de la Directive ne pouvait se limiter au dommage matériel et que, dès lors, il ne fallait pas tenir compte des restrictions prévues dans la loi anglaise transposant la Directive. ».

1563 Knetsch Jonas, « The compensation of non-pecuniary loss in GDPR infringement cases », 2022.

576. Précisions de la Cour de justice. Récemment, la Cour de Justice a précisé certains contours de la notion du dommage moral en matière de protection des données à caractère personnel[1564]. En effet, elle considère que le droit à réparation n'est pas réservé aux dommages moraux atteignant un certain seuil de gravité. Il s'agit d'une lecture stricte du règlement puisque ce dernier ne mentionne pas une telle condition et la Cour constate qu'une telle restriction contredirait la conception large des notions de dommage. De surcroît, elle considère que « subordonner la réparation d'un dommage moral à un certain seuil de gravité risquerait de nuire à la cohérence du régime instauré par le RGPD. En effet, la graduation dont dépendrait la possibilité ou non d'obtenir de la réparation serait susceptible de fluctuer en fonction de l'appréciation des juges saisis[1565]. ». Ainsi, pour cette affaire la Cour précise qu'un préjudice moral faible doit tout de même être réparé dès lors qu'il est tangible. En revanche, un préjudice insignifiant ou minime ne devra pas l'être : un simple sentiment d'inconfort ou un sentiment de contrariété n'équivaut pas à un dommage moral.

577. L'extension du dommage moral par la CJUE. Le 14 décembre 2023, la Cour de Justice a précisé que la crainte d'un potentiel usage abusif des données peut constituer un dommage moral susceptible d'être réparé sur le fondement de l'article 82 du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données[1566]. Dans cet arrêt, la Cour de Justice renforce les possibilités d'indemnisation pour les personnes concernées en estimant que la crainte d'un potentiel usage abusif à la suite d'une violation de données est susceptible à elle seule de caractériser un dommage moral. Par conséquent, la Cour de justice estime qu'il n'y a pas de différence entre le dommage moral relié à un usage abusif déjà produit ou la peur ressentie qu'un tel usage puisse se produire à l'avenir[1567]. L'interprétation extensive de la Cour de justice est indispensable pour permettre aux personnes concernées d'obtenir l'indemnisation de leurs préjudices.

[1564] Cour de justice de l'Union européenne, aff. C-300/21, 4 mai 2023, Österreichische Post ; Pailler Ludovic, « Quelle réparation pour le préjudice moral du fait d'une violation du droit de la protection des données ? », sur Dalloz Actualité, 2022.

[1565] *Ibid*., point 49.

[1566] Cour de Justice de l'Union européenne, aff. C-340-21, 14 décembre 2023.

[1567] Debet Anne, « La CJUE et le préjudice moral issu d'une violation de données », CCE, n° 2, février 2024 ; aff. précitée, point 81.

578. Les modalités d'évaluation. En matière d'évaluation des dommages et intérêts, le règlement prévoit que les personnes concernées doivent recevoir une réparation complète et effective pour le dommage subi[1568]. La référence au caractère « complet » de la réparation renvoie à la réparation intégrale, principe fondamental du droit de la responsabilité civile[1569]. La référence au caractère « effectif » de la réparation est plus incertaine, renvoyant sûrement au caractère réel de la réparation. Il s'agirait de prendre en compte le type de données à caractère personnel, la situation du demandeur, le caractère intentionnel du responsable de traitement, etc. La prise en compte de tous ces éléments - au cas par cas - permettrait une réparation effective[1570]. En pratique, il appartiendra donc aux juges nationaux de déterminer les critères de fixation des dommages et intérêts.

579. Les critères d'évaluation. En matière d'atteintes aux droits de la personnalité, les critères d'évaluation des dommages sont très complexes. Tout d'abord, il existe des divergences d'appréciation entre les États membres, le dommage moral faisant l'objet d'une appréciation subjective et cette divergence peut entraîner des phénomènes de *forum shopping* en matière de réparation[1571]. En effet, selon les juridictions nationales, les critères d'évaluation des dommages vont différer : certaines juridictions vont prendre en compte la situation de la victime mais également en compte le comportement du responsable de traitement[1572]. L'évaluation des dommages en identifiant la situation et le comportement du responsable de traitement est

[1568] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, considérant 146.

[1569] Brun Philippe, *Répertoire de droit civil*, éd. Dalloz, 2023 : Le principe de la réparation intégrale est un principe cardinal en droit de la responsabilité. De manière classique, la Cour de cassation énonce que « le propre de la responsabilité civile est de rétablir aussi exactement possible l'équilibre détruit par le dommage et de replacer la victime dans la situation où elle se serait trouvée si l'acte dommageable n'avait pas eu lieu (V. par exemple : Civ. 2e, 20 déc. 1966, Crim. 12 avr. 1994, no 93-82.579, Crim. 10 déc. 2013, no 13-80.954). La formule serait empruntée à Savatier René (*Traité de la responsabilité civile en droit français*, tome II, 2e éd., 1951, LGDJ, no 601).

[1570] Knetsch Jonas, *op. cit*.

[1571] Par exemple, certains États appliquent la théorie de la relativité aquilienne ; Sénat, Rapport d'information n° 558 (2008-2009) : « Plusieurs éléments contribuent à différencier le droit allemand du droit français sous l'angle de la responsabilité délictuelle : la modulation de la protection apportée en fonction de l'intérêt lésé, les atteintes corporelles bénéficiant d'un régime plus favorable ; la mise en balance des intérêts en présence ; l'exigence d'un rapport de causalité adéquat ; la "relativité aquilienne" qui correspond au fait que "l'action invoquant la responsabilité pour faute n'est admise que dans la mesure où le dommage invoqué est bien de la nature de celui qu'entendait prévenir la loi qui donne son caractère illicite au comportement du défendeur" ; ou encore la reconnaissance limité du préjudice moral qui ne peut en principe donner lieu à indemnisation que dans les cas prévus par une loi. ».

[1572] Knetsch Jonas, « Les actions civiles en réparation fondées sur une violation du RGPD : Vers un nouveau contentieux de masse ? », La Semaine Juridique Edition Générale, publié le 26 septembre 2022.

cohérente. Les géants du numérique ne doivent pas être sanctionnés de la même manière qu'une petite ou moyenne entreprise.

Par-delà les difficultés d'évaluation du dommage matériel et surtout moral, il existe des difficultés probatoires pour les victimes.

2. Les difficultés probatoires du préjudice

580. Un environnement diffus. Internet est un endroit « diffus », c'est-à-dire à la fois partout et à la fois nulle part. Il a certes besoin de câbles et de serveurs pour fonctionner, mais il n'existe pas un unique lieu de résidence pour Internet. La conséquence est la suivante : une action numérique à un endroit donné peut avoir des conséquences partout dans le monde[1573]. De surcroît, le caractère non rival des données permet à ces données de se trouver dans plusieurs endroits à la fois. Ainsi, il devient compliqué pour les individus de savoir où se trouvent leurs données à caractère personnel une fois communiquées à un organisme. Au regard de l'asymétrie d'information des personnes concernées, les individus ne sont généralement pas au conscient de l'utilisation de leurs données. Dans le meilleur des cas, lorsque les individus ont conscience de l'usage illicite de leurs données, il sera difficile pour eux de déterminer qui détient leurs données et où elles sont stockées.

581. La problématique récurrente des « boîtes noires ». De plus, l'environnement numérique complexifie l'apport de preuves tangibles par les victimes. Il sera complexe, voire impossible, pour un individu de prouver l'usage d'un algorithme par un établissement bancaire pour la détermination de son taux ou encore l'utilisation d'un algorithme discriminatoire pour l'obtention d'un emploi. L'opacité des algorithmes constitue une difficulté pour les individus dans un environnement où « les preuves disparaissent avec les changements d'algorithmes[1574] ».

[1573] Wylie Christopher et Blanchard Aurélien, *Mindfuck,* éd. Bernard Grasset, 2020, p. 436 : « Les crimes informatiques sont des crimes qui, en général, ne se produisent pas dans un lieu spécifique. Les crimes informatiques se comportent souvent comme la pollution, elle est partout de manière générale, et nulle part de manière spécifique. […] Même si de graves dommages sont commis, comme un hack, un vol de données, des menaces ou des tromperies, il est bien difficile de désigner le responsable, et nos systèmes existants d'évaluation des culpabilités et des reponsabilités ne sont tout simplement pas adaptés. ».

[1574] Toledano Joëlle, *GAFA : reprenons le pouvoir,* éd. Odile Jacob, 2020, p. 65 au sujet de Google : « D'après le Wall Street Journal, il y aurait eu, en 2018, 3 200 modifications de ses algorithmes de recherche, soit davantage qu'en 2017 avec 2 400 changements et "seulement" environ 500 en 2010 », (Grind Kirsten,

De surcroît, l'usage des procédés d'intelligence artificielle ne fait que renforcer l'opacité et l'absence de preuves. Avec l'intelligence artificielle, il devient presque impossible de déterminer quelles sont les données utilisées. En pratique, lorsque le responsable de traitement a pour obligation de supprimer les données litigieuses, il sera souvent dans l'impossibilité de respecter sa sanction.

Il existe également un manque de confiance envers ces acteurs : lorsque le responsable de traitement a l'obligation de supprimer les données, dans quelle mesure sommes-nous certains que ce dernier les a réellement supprimées[1575]. En effet, il est généralement plus intéressant pour le responsable de traitement de sauvegarder les données afin de pouvoir les réutiliser pour un usage ultérieur. En outre, lorsque le responsable de traitement a vendu les données à des tiers tels que des entreprises de courtage de données, il est quasiment impossible de retrouver la chaîne de tiers détenteurs de ces données. Ainsi, le régime de responsabilité demeure pour le moment « largement ineffectif en raison de la difficulté pour la victime de rapporter la preuve d'un préjudice[1576] ».

Schechner Sam, McMillan Robert et West John, « How Google interferes with its algorithms and changes your results », The Wall Street Journal, 15 novembre 2019).

[1575] Sur ce sujet, Monsieur Schrems a prouvé que Facebook conservait les données pourtant supprimées ; Leloup Damien « Facebook accusé de conserver des données effacées », Le Monde, 24 octobre 2011 : « À la lecture du document, M. Schrems a constaté que les informations qu'il avait effacées restaient stockées sur les serveurs de Facebook - notamment des messages privés dont le contenu pourrait lui porter préjudice. ».

[1576] Douville Thibaut, « La responsabilité des responsables du traitement et des sous-traitants à l'égard des personnes concernées : une grande oubliée », RAE, 2021, p. 34.

582. Conclusion de la section. L'effectivité d'un cadre normatif peut s'apprécier selon la volonté de sanctionner les acteurs qui ne respectent pas les principes du droit de la protection des données. Pour ce faire, il existe une diversité d'acteurs et de recours possibles afin de favoriser la prononciation des sanctions. En effet, la mise en place d'un partage de responsabilité entre le responsable de traitement et le sous-traitant permet d'améliorer l'indemnisation et l'aboutissement des actions des personnes concernées. Par ailleurs, l'inversion de la charge de la preuve renforce la possibilité pour les victimes d'obtenir réparation. Néanmoins, la diversité peut cependant devenir contreproductive en pratique : la mise en œuvre du cadre répressif s'avère complexe pour les personnes concernées.

L'environnement complexe et diffus d'internet ne permet pas de transposer les conditions de responsabilité civile classique. D'une part, le dommage moral en matière de protection de données à caractère personnel est difficile à évaluer. Il en ressort des divergences entre les juges nationaux, le dommage moral faisant l'objet d'une appréciation subjective. Les divergences entre les États membres mettent en péril l'objectif de cohérence du règlement européen. D'autre part, les dommages peuvent s'étaler ou survenir sur ou dans plusieurs années. Toutefois, il faut relever que la Cour de justice de l'Union européenne interprète strictement la responsabilité des responsables de traitement et largement la notion de dommage. La Cour de Justice rééquilibre les pouvoirs et affirme son rôle de garante de la cohérence du cadre normatif.

Pour autant, au regard du caractère non rival des données, les personnes concernées sont dans l'incapacité de déterminer où se trouvent les données ni qui les possèdent. L'absence de traçabilité des données met à mal l'opportunité pour les victimes d'obtenir une indemnisation suffisante. La mise en œuvre de l'action en indemnisation apparaît dès lors trop complexe pour les individus, souvent inconscients de l'usage illicite de leurs données à caractère personnel. Les traitements de données à caractère personnel sont souvent invisibles pour les individus concernés, permettant aux géants de numérique de faire prospérer leurs pratiques illicites.

Pour les raisons précitées, les actions en demande d'indemnisation de la part des individus sont encore rarissimes. À ce jour, seules les autorités nationales de contrôle sanctionnent certains acteurs pour leurs pratiques illicites. Il convient alors d'étudier l'action des autorités nationales afin d'appréhender l'effectivité du régime répressif.

Section 2 : L'inégale mise en œuvre du régime répressif par les différentes autorités de contrôle

583. Rôle des autorités administratives indépendantes. Afin de compenser les actions d'origine privées, les autorités nationales ont un rôle cardinal à jouer dans la mise en œuvre du régime répressif. Le système de sanctions prévu par le Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données repose en partie sur les sanctions administratives sous la direction des autorités de régulation. Ces dernières disposent d'un pouvoir de sanction « aux mille facettes[1577] », allant du simple rappel à l'ordre à d'imposantes sanctions.

584. Annonce du plan. La règle de droit devient effective lorsqu'elle est respectée par ses destinataires et sanctionnée par les autorités compétentes[1578] : les destinataires respectent les règles car les sanctions sont dissuasives et appliquées. Dès lors, il convient d'analyser la mise en œuvre variable des sanctions par les autorités nationales de contrôle (I). Néanmoins, au regard de la puissance des acteurs visés, quand bien même les sanctions sont appliquées, le montant s'avère fréquemment insuffisant (II).

[1577] Expression de Poullet Yves dans l'article « En marge d'un colloque : les sanctions au service du RGPD - une arme à double tranchant ? », CCE, n° 4, avril 2024.

[1578] En ce sens, v. Leroy Yann, « La notion d'effectivité du droit », Droit et société, n° 79, Éditions juridiques associées, 2011, p. 722 : « ce second postulat repose sur l'idée, liée à l'affirmation précédente, suivant laquelle toute norme juridique est accompagnée d'une sanction qui doit s'appliquer en cas de violation de la règle. La sanction serait le plus sûr moyen d'assurer le respect de la règle de droit et, par voie de conséquence dans ce raisonnement, la meilleure garantie de l'effectivité, la condition essentielle de son effectivité. […] Autrement dit, la fonction première de la sanction serait d'assurer l'effectivité d'une règle juridique, sa réalisation dans les faits. En ce sens, la sanction apparaît comme une condition essentielle de l'effectivité d'une norme juridique puisque la menace de son prononcé est érigée en élément crucial dans l'attitude des sujets de droit face à l'obligation posée ; ou, pour le dire autrement, elle est le moyen de rétablir l'effectivité du droit lorsque celui-ci a été violé. Il est alors couramment affirmé le rapport évident entre le taux de conformité à une norme juridique et la sévérité de la sanction prévue en cas de violation de celle-ci. » ; en matière de protection des données à caractère personnel : Martial-Braz Nathalie, Rochfled Judith, Gattone Emilie, « Quel avenir pour la protection des données à caractère personnel en Europe ? Les enjeux de l'élaboration chaotique du règlement relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données », Recueil Dalloz, 2013, 2788.

I. L'intensification variable de l'activité répressive des autorités de contrôle

585. Méthode d'appréciation. Les amendes administratives sont indispensables aux autorités de contrôle pour faire respecter le règlement européen. À ces fins, les autorités doivent appliquer les amendes de manière cohérente et harmonisée au sein de l'Union européenne. Il convient d'analyser la méthode d'appréciation des sanctions (A) ainsi que sa mise en œuvre par les autorités de contrôle (B).

A) L'appréciation variable des sanctions

586. Approche subjective. Le règlement européen prévoit une appréciation des sanctions au cas par cas afin d'adapter le montant de l'amende à chaque acteur (1). Par ailleurs, le Comité de protection des données confirme la volonté d'une cohérence des sanctions en établissant une méthode de calcul (2).

1. Une appréciation variable

587. Une sanction harmonisée. Afin d'éviter les divergences d'appréciation des sanctions par les autorités de contrôle, le règlement européen prévoit des conditions générales pour l'imposition des amendes administratives. L'article 83 du règlement prévoit dans un premier temps que les sanctions doivent être effectives, proportionnées et dissuasives. La triade employée par le règlement européen illustre le changement de paradigme du régime répressif en matière de protection des données à caractère personnel : les sanctions doivent être appliquées réellement et être d'un montant suffisamment élevé en fonction de chaque acteur. Ainsi, chaque amende administrative devra être appréciée en tenant compte de la nature, de la gravité, de la durée de la violation et des catégories de données à caractère personnel concernées par la violation. Le comportement du responsable de traitement aura également son importance au regard des mesures prises *a posteriori* afin d'atténuer le dommage subi par les personnes concernées, des possibles violations commises précédemment ou encore sa coopération établie avec l'autorité de contrôle. Enfin, le potentiel avantage financier du fait de la violation sera autant pris en compte.

588. Une appréciation au cas par cas. Ainsi, le règlement européen instaure une méthode de calcul comprenant plusieurs éléments à prendre en compte afin d'établir le montant proportionné à l'atteinte. L'appréciation au cas par cas permet d'adapter le montant de l'amende administrative à chaque acteur[1579]. Il est louable d'avoir augmenté drastiquement le montant des sanctions afin de s'adapter *a minima* à la puissance des géants du numérique. Le caractère « dissuasif » des sanctions semble respecté à la lecture du règlement. En effet, le règlement prévoit que le montant des amendes administratives peut s'élever jusqu'à 20 000 000 euros et dans le cas d'une entreprise, jusqu'à 4% du chiffre d'affaires annuel mondial total de l'exercice précédent[1580]. Avant l'entrée en vigueur du règlement européen, le montant maximal des sanctions était de 150 000 euros maximum[1581]. Pour des entreprises d'une telle ampleur que les géants du numérique, le montant des sanctions était dérisoire et n'avait aucun effet dissuasif. À titre d'illustration, en mai 2017, Facebook avait été condamné à hauteur de 150 000 euros[1582]. La sanction équivalait à 0,005% du dernier bénéfice trimestriel de la société, soit l'équivalent de moins de trente minutes de son activité économique[1583] : les sanctions n'étaient nullement dissuasives. L'augmentation du montant des sanctions était donc nécessaire afin de renforcer l'effectivité du cadre répressif par les autorités de contrôle.

Néanmoins, l'adaptation du montant des sanctions apparaît nécessaire afin de ne pas infliger des sanctions équivalentes à un géant du numérique ou à une petite ou moyenne entreprise. Tout d'abord, les petites et moyennes entreprises n'ont pas les mêmes ressources en matière de

---

1579 Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, considérant 29 : « Les pouvoirs des autorités de contrôle devraient être exercés conformément aux garanties procédurales appropriées prévues par le droit de l'Union et le droit des États membres, d'une manière impartiale et équitable et dans un délai raisonnable. Toute mesure devrait notamment être appropriée, nécessaire et proportionnée en vue de garantir le respect du présent règlement, compte tenu des circonstances de l'espèce. ».

1580 Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, articles 83-4, 83-5 et 83-6.

1581 Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, article 47, paragraphe 2 (version en vigueur du 31 mars 2011 au 9 octobre 2016, modifié par la loi n°2011-334 du 29 mars 2011 - art. 8) : « Lors du premier manquement, il ne peut excéder 150 000 euros. En cas de manquement réitéré dans les cinq années à compter de la date à laquelle la sanction pécuniaire précédemment prononcée est devenue définitive, il ne peut excéder 300 000 euros ou, s'agissant d'une entreprise, 5 % du chiffre d'affaires hors taxes du dernier exercice clos dans la limite de 300 000 euros. ». La loi n° 2016-1321 pour une République numérique avait augmenté le montant à 3 000 000 d'euros.

1582 CNIL, délibération de la formation restreinte n° SAN-2017-00627, avril 2017.

1583 Chignard Simon et Benyayer Louis-David, *Datanomics*, éd. FYP, 2015, p. 146 ; Basdevant Adrien « Après l'amende infligée à Facebook, les utilisateurs sont-ils mieux protégés ? », interview de Laurence Neuer, Le point, 27 mai 2017.

données à caractère personnel. En outre, aucune entreprise ne pourra rivaliser avec les expérimentations faites par les géants du numérique sur les données à caractère personnel de leurs utilisateurs. Ils ont acquis une base de données sans précédent, ce qui n'est pas forcément le cas des autres entreprises. Ainsi, le non-respect des obligations par une petite ou moyenne entreprise n'aura pas le même impact qu'une violation du règlement par les géants du numérique.

589. Violation commise délibérément. Par ailleurs, les autorités de contrôle doivent prendre en compte « l'intention » du responsable de traitement ou du sous-traitant de commettre la violation. De manière appropriée, les violations commises délibérément seront sanctionnées plus sévèrement du fait de leur mépris des dispositions législatives[1584]. À titre d'illustration, la vente de données à caractère personnel à des fins de commercialisation sans le consentement de la personne concernée constitue une violation commise délibérément par le responsable de traitement. Cette pratique est courante auprès des géants du numérique qui n'hésitent pas à vendre les données à des courtiers de données. Malheureusement, il est usuellement difficile de prouver la vente de ses données au regard du caractère difficilement traçable des données.

Malgré les difficultés pratiques, les autorités de contrôle disposent de moyens renforcés afin de détecter les violations par les responsables de traitement. Afin d'estimer le montant des amendes de manière cohérente, le CEPD propose une méthode de calcul harmonisée.

2. Une appréciation cohérente

590. Méthode de calcul. Dans le dessein d'harmoniser la méthode utilisée par les autorités de contrôle lors du calcul de l'amende, les lignes directrices concernant la méthode de calcul des amendes administratives ont été définitivement adoptées le 24 mai 2023 après une période de consultation publique[1585]. Les lignes directrices vont établir des points de départ en relevant plusieurs éléments devant être pris en compte : la catégorisation des infractions par nature, la gravité de l'infraction et le chiffre d'affaires de l'entreprise. Suite à ce point de départ, le Comité européen de la protection des données élabore une méthodologie composée de cinq étapes pour

[1584] Groupe de travail sur l'article 29 (G29), « Lignes directrices sur l'application et la fixation des amendes administratives aux fins du règlement (UE) 2016/679 », WP253, adoptées le 3 octobre 2017.
[1585] Comité européen de protection des données (CEPD), « Lignes directrices 04/2022 sur le calcul des amendes administratives », version 2.1, adoptées le mardi 24 mai 2023.

le calcul des amendes administratives. Premièrement il s'agit d'identifier les comportements afin de déterminer s'il s'agit d'un comportement sanctionnable par le règlement[1586]. Deuxièmement, les autorités doivent se fonder sur un point de départ en classifiant l'infraction, en évaluant sa gravité et en prenant en compte le chiffre d'affaires de l'entreprise. Troisièmement, les autorités doivent tenir compte des circonstances aggravantes ou atténuantes liées au comportement passé ou présent du responsable de traitement et/ou sous-traitant susceptibles d'augmenter ou de diminuer le montant de l'amende. La quatrième étape consiste à déterminer les plafonds légaux des amendes afin de ne pas dépasser le montant maximum. Pour finir, les autorités de contrôle doivent analyser le montant final au regard des exigences d'effectivité, de dissuasion et de proportionnalité. En fonction de cette analyse, le montant peut être ajusté.

591. Méthode subjective. En revanche, le CEPD rappelle dans ses lignes directrices qu'il s'agit surtout d'une analyse en fonction des circonstances et non simplement un calcul mathématique[1587]. Les autorités de contrôle ne sont pas soumises à cette méthode lorsque les étapes ne sont pas appliques en l'espèce. En revanche, le raisonnement devra inclure le niveau de gravité, le chiffre d'affaires de l'entreprise et les facteurs atténuants ou aggravants qui ont été appliqués. Ainsi, les autorités de contrôle doivent logiquement analyser chaque cas d'espèce en fonction des critères précités. Le montant final de l'amende administrative ne devra être ni trop élevé au risque d'affaiblir les entreprises, ni trop limité au risque de décrédibiliser les autorités de contrôle : la détermination du montant ne pourra jamais être une « science exacte[1588] ». En revanche, le fait que les géants du numérique perpétuent leurs pratiques nous semble être un indicateur quant à l'insuffisance des montants infligés.

Par ailleurs, il existe des disparités d'application entre les différentes autorités de contrôle, réduisant la crédibilité de ces autorités aux yeux des acteurs du numérique.

1586 Plus précisément l'article 83.3 du RGPD.

1587 *Ibid.*, p. 7 : « The aim of these Guidelines is to create harmonised starting points as a common orientation, on the basis of which the calculation of administrative fines in individual cases can take place. However, it is settled case law that any such guidance need not be as specific as to allow a controller or processor to make a precise mathematical calculation of the expected fine. It is emphasised throughout these Guidelines that the final amount of the fine depends on all the circumstances of the case. The EDPB therefore envisages harmonisation on the starting points and methodology used to calculate a fine, rather than harmonisation on the outcome. ».

1588 Netter Emmanuel, « Du simple au décuple. Hésitations autour de la juste proportion des sanctions en droit des données personnelles : le cas Accord », Dalloz, 575.

B) Les disparités d'application des sanctions

592. Disparités d'application. Lorsque le montant de l'amende administrative est déterminé, les sanctions doivent être prononcées et respectées. En France, la Commission nationale de l'informatique et des libertés exerce son rôle d'autorité de contrôle depuis 1978. L'autorité de contrôle nationale a renforcé son action de manière affirmée (1), tandis que certains de ses homologues freinent leur action au regard d'une certaine dépendance économique (2).

1. L'action affirmée de la Commission nationale de l'informatique et des libertés

593. Bilans de la Commission nationale de l'informatique et des libertés. Dans son bilan de 2022[1589], la CNIL liste ses actions avec 345 contrôles réalisés, 147 mises en demeure notifiées et 21 sanctions adoptées pour un total cumulé de plus de 100 millions d'euros[1590]. L'autorité de contrôle nationale rappelle toutefois son objectif principal : la mise en conformité avant la sanction. En effet, selon elle, 94% des investigations menées auprès des organismes aboutissent à une mise en conformité sans amende administrative. Néanmoins, depuis l'entrée en vigueur du règlement européen, la Commission nationale de l'informatique et des libertés a prononcé plus d'un demi-milliard d'euros d'amende. Le montant des sanctions reflète l'importance des données dans les modèles d'affaires actuels. Pour 2023, la Commission nationale de l'informatique et des libertés réaffirme sa politique avec un doublement significatif des sanctions : 42 sanctions dont 18 en procédure ordinaire et 24 en procédure simplifiée[1591]. Le total du montant des sanctions en 2023 s'élève à 89 179 500 euros.

594. Sanctions nationales de la CNIL. La Commission nationale de l'informatique et des libertés a pour mission de contrôler et de sanctionner les opérateurs institutionnels français qui ne respectent pas la législation en matière de protection de données à caractère personnel. À titre d'illustration, l'autorité de contrôle nationale a sanctionné Infogreffe à une sanction de 250 000 euros pour manquement en matière de durées de conservation et de sécurité des données à caractère personnel[1592]. La durée de conservation indiquée sur le site n'était pas réellement

[1589] Commission nationale de l'informatique et des libertés, « Rapport annuel 2022 », publié le 23 mai 2023.
[1590] 101 277 900 euros plus précisément.
[1591] Commission nationale de l'informatique et des libertés, « Rapport annuel 2023 », publié le 23 avril 2024.
[1592] Commission nationale de l'informatique et des libertés, délibération de la formation restreinte n° SAN-2022-018, 8 septembre 2022 concernant le "GIE Infogreffe".

respectée puisque les données de 25% des utilisateurs faisaient l'objet d'une durée de conservation au-delà des délais indiqués. De surcroît, le site n'imposait pas la création d'un mot de passe robuste et transmettait et conservait en clair les mots de passe non temporaires. Ainsi, le registre du commerce et des sociétés n'a pas respecté l'obligation de conserver les données pour une durée proportionnée à la finalité du traitement[1593] et l'obligation d'assurer la sécurité des données personnelles[1594].

Sans surprise, de nombreux manquements au règlement européen proviennent des activités de courtage. En effet, la Commission nationale de l'informatique et des libertés a relevé l'absence d'information sur l'identité des partenaires lors des opérations de prospection. Lorsque les données font l'objet de transmissions successives à plusieurs tiers, les courtiers ne sollicitent pas à nouveau le consentement des personnes concernées. Surtout, dans les cas les plus graves, les données sont transmises à des partenaires commerciaux à des fins de prospection en l'absence de toute information pour les individus[1595]. À ce sujet, la Commission nationale de l'informatique et des libertés a prononcé une sanction de 600 000 euros à l'encontre du groupe hôtelier Accor pour avoir procédé à la prospection commerciale sans le consentement des personnes concernées[1596]. En effet, l'autorité de contrôle a constaté que lorsqu'une personne procédait à une réservation sur le site de l'hôtel, elle était automatiquement destinataire d'une newsletter comportant des offres commerciales de partenaires, la case relative au consentement de cette newsletter était précochée par défaut[1597]. À l'instar de la société Accor, l'autorité de

1593 Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, article 5.1. e) : « conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées ; les données à caractère personnel peuvent être conservées pour des durées plus longues dans la mesure où elles seront traitées exclusivement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques conformément à l'article 89, paragraphe 1, pour autant que soient mises en œuvre les mesures techniques et organisationnelles appropriées requises par le présent règlement afin de garantir les droits et libertés de la personne concernée (limitation de la conservation) ».

1594 Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, article 32.

1595 Commission nationale de l'informatique et des libertés, « Rapport annuel 2022 », p. 79.

1596 Commission nationale de l'informatique et des libertés, délibération de la formation restreinte n° SAN-2022-017 du 3 août 2022 concernant la société "Accor SA" ; Commission nationale de l'informatique et des libertés, « Prospection commerciale et droits des personnes : sanction de 600 000 euros à l'encontre d'Accor », 17 août 2022.

1597 Plusieurs autres manquements ont été constatés tels qu'un manquement à l'obligation d'informer les personnes (articles 12 et 13 du RGPD), un manquement à l'obligation de respecter le droit d'accès des personnes aux données les concernant (articles 12 et 15 du RGPD), un manquement à l'obligation de respecter le droit d'opposition des personnes concernées (article 12 et 21 du RGPD), et un manquement à l'obligation d'assurer la sécurité des données personnelles (article 32 du RGPD) ; Pour le calcul de l'amende,

contrôle nationale a également sanctionné quelques mois plus tard la société « EDF » pour ne pas avoir respecté ses obligations en matière de prospection commerciale[1598].

Ainsi, les sanctions envers les organismes français se comptent en centaine de milliers d'euros. L'autorité de contrôle nationale évalue au cas par cas les manquements en prenant en considération l'importance de l'organisme contrôlé. Néanmoins, elle n'hésite pas à infliger des sanctions se comptant en millions si nécessaire même pour les entreprises françaises. Le 15 juin 2023, la Commission nationale de l'informatique et des libertés a condamné la société « Criteo » à un montant de 40 millions d'euros pour ne pas avoir vérifié que les personnes dont elle traite les données avaient donné leur consentement[1599]. Le 29 décembre 2023, l'autorité de régulation a sanctionné la société « Amazon France Logistique » d'une amende de 32 millions, notamment pour avoir mis en place un système de surveillance de l'activité et des performances des salariés « excessivement intrusif[1600]». Les sanctions concernant les géants du numérique sont rationnellement plus élevées au regard de la puissance financière de ces acteurs.

595. Sanction « historique » contre Google. L'autorité de contrôle nationale a condamné plusieurs géants du numérique par des sanctions en millions d'euros. Dès 2019, soit un an après l'entrée en vigueur du règlement européen, l'autorité de contrôle nationale va faire usage de son considérable pouvoir de sanction auprès des géants du numérique[1601]. L'autorité de contrôle va démontrer sa crédibilité avec une amende qualifiée « d'historique[1602] » en janvier 2019

au sujet du caractère dissuasif : Netter Emmanuel, op. cit. : « De l'avis de l'EDPB, un tel montant [100 000 euros] ne découragerait pas Accor et d'autres entreprises de commettre des infractions "substantielles" similaires, et encore moins de commettre des infractions moins "substantielles", étant donné que le risque encouru en cas de telles infractions serait une sanction dérisoire au regard de leur taille économique. Cette motivation nous paraît pleinement convaincante. Elle a conduit le CEPD à adopter une « décision contraignante » obligeant la CNIL à réévaluer son projet de décision. Dans sa délibération du 3 août, la CNIL "prend acte" de la décision contraignante et réévalue à 600 000 € le montant de l'amende prononcée ».

[1598] Délibération de la formation restreinte n°SAN-2022-021 du 24 novembre 2022 concernant la société "Électricité de France" ; Commission nationale de l'informatique et des libertés, « Prospection commerciale et droits des personnes : sanction de 600 000 euros à l'encontre d'EDF », 29 novembre 2022.

[1599] Berezkina Ekaterina, « Cookies : la CNIL précise les obligations de contrôle de conformité entre responsables de traitement conjoints », Dalloz IP/IT, 2023, p. 383 ; CNIL, 15 juin 2023, n° SAN-2023-009.

[1600]Commission nationale de l'informatique et des libertés, délibération n° SAN-2023-021, 27 décembre 2023.

[1601] Gavard Emmanuel, « La CNIL change de ton avec les entreprises de la tech », Stratégies, publié le 16 janvier 2023.

[1602] Netter Emmanuel, « Sanction à 50 millions d'euros : au-delà de Google, la CNIL s'attaque aux politiques de confidentialité obscures et aux consentements creux », Dalloz IP/IT, 2019, p. 165 : « Il est rare qu'une

puisque la société Google va être condamnée à une amende record de 50 millions d'euros faisant l'objet d'un fort écho médiatique[1603]. En l'espèce, la Commission nationale de l'informatique et des libertés va constater un manquement continu des obligations de transparence et d'information lors de la collecte de données à caractère personnel, violant ainsi les droits des personnes ainsi qu'une absence de base légale pour les traitements de personnalisation de publicité[1604]. Par conséquent, la formation restreinte de la CNIL considère qu'il s'agit d'une sanction pécuniaire justifiée compte tenu de la place prépondérante occupée par la société.

596. Recours devant le Conseil d'État. Au contraire, la société Google va contester la décision dans le cadre d'un recours devant le Conseil d'État. Pour autant, le Conseil d'État confirme le manquement à l'obligation d'information ainsi que l'absence de recueil d'un consentement libre et éclairé pour les utilisateurs[1605]. La juridiction administrative suprême estime que le montant de la sanction n'est pas disproportionné au regard de la gravité des manquements, de leur caractère continu et de leur durée[1606]. Cette sanction marque le changement de paradigme opéré par l'autorité de contrôle nationale puisque la sanction a été prononcée sans mise en demeure préalable du responsable de traitement.

597. Intensification des contrôles. De surcroît, la Commission nationale de l'informatique et des libertés va intensifier les contrôles afin de mettre en œuvre effectivement son pouvoir de sanction. Toujours contre Google - deux ans plus tard - la Commission nationale de l'informatique et des libertés va cette fois-ci prononcer une sanction de 150 millions d'euros au

décision mérite qu'on la qualifie « d'historique », sans que ce terme soit en rien galvaudé. Tel est le cas de cette délibération, dont on dira encore dans plusieurs années qu'elle a constitué un tournant. ».

[1603] Ronfault Lucie « RGPD : la CNIL impose à Google une sanction record de 50 millions d'euros », Le Figaro, 21 janvier 2019 ; « Protection des données : La CNIL inflige une amende record de 50 millions d'euros à Google », Le Parisien, 21 janvier 2019 ; Dumoulin Sébastien, « RGPD : la CNIL inflige une amende historique à Google », Les Echos, 21 janvier 2019 ; « Untersinger Martin, « La condamnation de Google à 50 millions d'euros d'amende confirmée par le Conseil d'Etat », Le Monde, 19 juin 2020 ; etc.

[1604] Commission nationale de l'informatique et des libertés, délibération n° SAN-2019-001, 21 janvier 2019.

[1605] Conseil d'État, n°430810, 19 juin 2020, publié au recueil Lebon.

[1606] *Ibid*., point 27 : « Il résulte de ce qui précède qu'eu égard à la gravité particulière des manquements commis, qui tient à la nature des exigences méconnues et à leurs effets sur les utilisateurs, au caractère continu de ces manquements et à la durée de la période durant laquelle ils ont perduré, aux plafonds prévus par le 4 de l'article 83 du RGPD, et à la situation financière de la société, la sanction pécuniaire de 50 000 000 d'euros prononcée à l'encontre de la société Google ne revêt pas un caractère disproportionné ».

sujet des *cookies*[1607]. Le principe à respecter est élémentaire : il doit être permis aux utilisateurs de refuser les cookies aussi facilement que de les accepter. La CNIL justifie le montant de la sanction au regard du nombre de personnes concernées et par les bénéfices considérables que la société tire des revenus publicitaires grâce aux *cookies*. Au sujet des *cookies*, l'autorité de régulation nationale a également condamné la société Microsoft à 60 millions d'euros pour ses pratiques[1608]. En effet, le système mis en place par la société déposait automatiquement des *cookies* sur le terminal de l'utilisateur, sans le recueil préalable de son consentement. Par ailleurs, la CNIL a également constaté l'absence de mécanisme permettant de refuser les *cookies* aussi facilement que de les accepter. Les agissements de la société relèvent des pratiques de manipulation courantes par les géants du numérique. L'autorité de contrôle nationale a donc considéré que le montant de la sanction administrative était proportionné au regard de la puissance de la société et des revenus tirés de cette pratique. D'autres géants du numérique ont été condamnés pour des pratiques similaires, tels que la société « Amazon » pour un montant de 35 millions[1609] ou encore « TikTok » pour un montant de 5 millions d'euros[1610].

[1607] Netter Emmanuel, « "Refuser tous les cookies". Espoirs et mirages d'une régulation par les boutons », Dalloz IP/IT 2022, p. 392 ; Commission nationale de l'informatique et des libertés, Délibération de la formation restreinte n° SAN-2021-023 du 31 décembre 2021 concernant les sociétés Google LLC et Google Ireland Limited.

[1608] Boullier Valentin, « CNIL et Microsoft : délibération du 11 mai 2023 clôturant l'injonction faite par la CNIL à Microsoft le 19 décembre 2022 en matière de cookies », Dalloz Actualité, 16 juin 2023 : « Concernant plus particulièrement les modalités de recueil de ce consentement, la CNIL avait pu relever que le bandeau cookies s'affichant sur bing.com permettait d'accepter les cookies de manière immédiate, mais qu'aucune fonctionnalité similaire ne permettait de refuser les cookies. Pour ce faire, il était nécessaire, de cliquer sur "Plus d'options", puis sur "Enregistrer" les paramètres. Il existait donc un déséquilibre entre le refus et l'acceptation, cette seconde étant plus aisée, car sollicitant moins l'utilisateur du moteur de recherche. » ; CNIL, Délibération de la formation restreinte n° SAN-2022-023 du 19 décembre 2022 concernant la société Microsoft Ireland Operations Limited.

[1609]Commission nationale de l'informatique et des libertés, délibération n° SAN-2020-013, 7 décembre 2020, décision validée par le Conseil d'État, décision n° 451423 ; Hardouin-Ayrinhac Marie-Lou, « Cookies : sanction de 35 millions d'euros à l'encontre d'Amazon Europe Core », Le Quotidien, décembre 2020 : « La formation restreinte a relevé que lorsqu'un internaute se rendait sur l'une des pages du site " amazon.fr", un grand nombre de cookies à vocation publicitaire était instantanément déposé sur son ordinateur, c'est-à-dire avant que celui-ci n'exécute la moindre action. ».

[1610] Commission nationale de l'informatique et des libertés, Délibération de la formation restreinte n° SAN-2022-027 du 29 décembre 2022 concernant les sociétés Tiktok information technologies UK Limited et Tiktok Technology Limited : « Lors du contrôle effectué en juin 2021, la CNIL a constaté que si les sociétés Tiktok Royaume-Uni et Tiktok Irlande proposaient bien un bouton permettant d'accepter immédiatement les cookies, elles ne mettaient pas en place de solution équivalente (bouton ou autre) pour permettre à l'internaute de refuser aussi facilement leur dépôt. Plusieurs clics étaient nécessaires pour refuser tous les cookies, contre un seul pour les accepter. ».

2. L'action inégale des homologues de la CNIL

598. Intensification répressive des autorités. Depuis l'entrée en vigueur du règlement européen, certaines homologues de la CNIL n'ont pas hésité à sanctionner les géants du numérique[1611]. En effet, suite à la condamnation par la CNIL en 2020 d'Amazon pour un montant de 35 millions d'euros, l'autorité luxembourgeoise de la protection des données à caractère personnel a prononcé une sanction de 746 millions à son encontre pour ses pratiques de ciblage publicitaire imposé aux personnes concernées[1612]. La Commission nationale de l'informatique et des libertés irlandaise quant à elle a infligé une amende record d'un montant d'1,2 milliards d'euros à la société Facebook[1613]. Il s'agit de l'amende la plus conséquente dans la mise en œuvre du droit européen de la protection des données à caractère personnel. Le régulateur irlandais reproche à Facebook d'avoir continué à transférer des données à caractère personnel des utilisateurs européens vers les Etats-Unis malgré l'invalidation par la Cour de Justice de l'Union européenne[1614].

599. Le mécanisme de guichet unique. En réalité, les sanctions conséquentes de l'autorité irlandaise et luxembourgeoise ont été adoptées en vertu du mécanisme du guichet unique, et souvent après l'arbitrage du Comité européen de la protection des données. En effet, les autorités précitées auraient préféré régler les manquements à l'amiable afin de demeurer un État attractif pour ces acteurs. À l'instar de la CNIL, ses homologues font usage de leur pouvoir de sanction afin de rendre effectif la protection des personnes concernées. En vertu du mécanisme de guichet unique, l'autorité de protection des données du pays où se situe l'établissement

---

1611 Botchorichvili Nana « Bilan des sanctions prononcées par les autorités européennes de protection des données : quelles tendances ? », CCE, n° 3, mars 2024 : « On dénombre depuis le 25 mai 2018 autour de 6 680 sanctions financières prononcées par l'ensemble des autorités européennes pour un montant total de plus de 4 billions d'euros en cumulé, avec des autorités de protection des données plus actives que d'autres en la matière. Tel est le cas de l'autorité espagnole qui avec 1 596 sanctions financières prononcées se positionne, parmi ses homologues, avec un des plus hauts palmarès. Elle est suivie par les autorités italienne, bulgare et hongroise avec respectivement 598, 310 et 209 sanctions financières relevées. ».

1612 Commission nationale de l'informatique et des libertés, « L'autorité luxembourgeoise de protection des données a prononcé à l'encontre d'Amazon Europe Core une amende de 746 millions d'euros », 3 août 2021, disponible en ligne.

1613 Schmitt Fabienne, « Meta écope d'une amende record de 1,2 milliard pour transfert illégal de données », Le Figaro, publié le 22 mai 2023 ; Untersinger Martin et Clairouin Olivier, « Meta condamné à une amende record de 1,2 milliards d'euros par le régulateur irlandais des données personnelles », Le Monde, 22 mai 2023.

1614 Cour de Justice de l'Union européenne, aff. DPC c/ Facebook Ireland Ltd et M. Schrems, juillet 2020 ; Crichton Cécile, « Transfert de données vers les USA : l'arrêt Schrems II », 22 juillet 2020, Dalloz actualité.

principal d'une société devient l'interlocutrice privilégiée. L'autorité de protection devient l'autorité dite « chef de file » chargée de mener des actions de contrôle et si nécessaire, des actions répressives. Le mécanisme permettrait d'assurer une application cohérente du régime répressif au sein de l'Union européenne.

600. Risques du mécanisme. En réalité, le mécanisme de guichet unique favorise le *forum shopping* et le *regulatory shopping* puisque les très grandes plateformes sont installées dans les États membres les plus indulgents concernant la fiscalité et le contrôle des pratiques en matière de protection des données à caractère personnel[1615]. La problématique réside dans « l'appétence des grandes entreprises du numérique pour le guichet unique[1616] ». En effet, les disparités de politiques fiscales entre les États membres permettent à certains États d'être attractifs pour les géants du numérique[1617] : la plupart des géants du numérique ont leur établissement principal ou unique en Irlande ou au Luxembourg : les établissements d'Alphabet (Google et Youtube), Meta (Facebook, Instagram et WhatsApp) ou encore de Microsoft se situent en Irlande et la société Amazon a choisi le Luxembourg pour son établissement principal. Ils implantent leurs sièges sociaux dans les États membres où le taux est évidemment le plus faible. Dès lors, l'optimisation fiscale leur permet d'accumuler une somme colossale d'argent faisant l'objet de réserve en cas de sanction[1618]. *In fine*, la politique des États membres devient favorable pour ces acteurs du numérique : « la règle se négocie, la localisation géographique des entreprises et des contrats se choisit en fonction des facilités offertes par les législations et juridictions respectives

[1615] Vergnolle Suzanne, *L'effectivité de la protection des personnes par le droit des données à caractère personnel*, éd. Larcier, 2022, p. 427 ; Toledano Joëlle, *GAFA, reprenons le pouvoir*, éd. Odile Jacob, 2020, p. 98 : « Vertueuse dans son principe, la règle a aussi des effets pervers en particulier quand les entreprises non européennes viennent s'installer en Europe : on peut craindre qu'une entreprise ne choisisse son lieu d'installation qu'en fonction du régime de réglementation auquel elle sera exposée. Le choix risque de se porter sur le régime le moins couteux ou le moins exigeant. Et les décideurs, pour attirer de nouveaux acteurs, sont susceptibles d'élaborer une réglementation qui convienne à ses entreprises. C'est effectivement le cas s'agissant des services numériques : la TVA du Luxembourg, la plus basse parmi les pays européens s'est avérée très attractive pour Amazon, la possibilité de négocier la politique directe en Irlande a séduit Apple, comme d'ailleurs les faibles exigences et moyens du régulateur irlandais sur le contrôle des données à caractère personnel ont facilité l'installation de Facebook en Europe. ».

[1616] Pouillaude Sibylle, « "Attraper les GAFAM" ou le guichet unique en droit de la protection des données personnelles : fonctionnement, bilan et perspectives », Revue du droit de l'Union européenne, 2023, p. 140.

[1617] Grange Maryline, « Internet rattrapé par le droit », Politique étrangère, Institut français des relations internationales, 2019.

[1618] Smyrnaios Nikos, « L'effet GAFAM : stratégies et logiques de l'oligopole de l'internet », Communication et langages, 188, 2016.

des États mis en concurrence[1619] ». À nouveau, leur influence leur permet de contourner les règles.

601. Les manquements de la Commission irlandaise. Pire encore, les acteurs du numérique peuvent bénéficier de la clémence de l'autorité de régulation irlandaise. En effet, avec le mécanisme du guichet unique, la plupart des manquements des géants du numérique devraient être sanctionnés par le régulateur irlandais. Néanmoins, sa politique économique rend la Commission irlandaise très dépendante des plateformes[1620]. Un rapport publié le 15 mai 2023 par une ONG de défense des libertés publiques décrit l'autorité de régulation irlandaise comme un « goulot d'étranglement des procédures »[1621]. En effet, l'ONG rapporte que depuis 2018, sur 54 dossiers instruits, la Commission irlandaise a conclu des accords à l'amiable dans 46 cas, ce qui correspond à seulement 8 procédures de sanctions sur les 54 dossiers[1622]. En réalité, l'autorité irlandaise est le seul régulateur à avoir recours massivement aux procédures amiables. Le recours massif à des accords amiables est contestable pour les entreprises ayant déjà été condamnées par le passé. Le règlement européen avait pourtant renforcé les pouvoirs de sanctions des autorités afin de rendre effectif le cadre normatif. En réalité, l'autorité de contrôle irlandaise brille par son « laxisme »[1623]. En 2021, le Parlement européen avait soulevé son inquiétude sur les actions répressives « inégales et parfois inexistantes », particulièrement des autorités irlandaise et luxembourgeoise[1624]. Récemment, le 10 septembre 2024, la Cour de Justice a donné un signal assez fort contre les avantages fiscaux octroyés par l'Irlande : Apple a été condamné à rembourser 13 milliards d'euros à cet État[1625]. La Cour de Justice précise que

[1619] Ost François et Kerchove Michel van de, « De la pyramide au réseau ? », Revue interdisciplinaire d'études juridiques, Volume 44, 2000, p. 81.

[1620] Bouckaert Colette et Cavada Jean-Marie, « L'Irlande est-elle un frein à l'application du RGPD en Europe ? », IDFRights, publié le 13 juin 2023 ; Vinocur Nicholas « We have a huge problem : European tech regulator despairs over lack of enforcement », Politico, 28 décembre 2019 : « Ireland and Luxembourg have faced special scrutiny because so many U.S. tech companies have set up shop in those tiny nations, which have actively courted them thanks to a mix of low corporate tax rates and business-friendly regulation. Those close relationships have created a strong degree of economic dependency, particularly in the Irish case, which raises questions as to whether these countries are best suited to regulating Big Tech. ».

[1621] Irish Council for Civil Liberties, Rapport « 5 years : GDPR's crisis point », 2023.

[1622] Leloup Damien, « Cinq ans après le RGPD, des GAFAM ménagés par la CNIL irlandaise », Le Monde, 14 mai 2023.

[1623] Netter Emmanuel, « Du simple au décuple. Hésitations autour de la juste proportion des sanctions en droit des données personnelles : le cas Accor », RTD com., 2022, 575.

[1624] Nana Botchorichvili, « Faut-il réviser le RGPD ? », Dalloz IP/IT, 2023, 499 ; Parlement européen, Résolution concernant le rapport d'évaluation de la Commission sur la mise en œuvre du règlement général sur la protection des données deux ans après son entrée en application, 2020/271 (RSP), 25 mars 2021.

[1625] Cour de Justice de l'Union européenne, aff. n° C-465/20, 10 septembre 2024.

la société Apple avait bénéficié de rescrits fiscaux ayant « artificiellement réduit les impôts ». À nouveau, la Cour de Justice permet de rétablir une certaine cohérence et un équilibre entre les pays membres afin que le mécanisme du guichet unique soit efficace.

602. Montant relativement faible des amendes. Pour autant, lorsque l'autorité décide d'aboutir à des sanctions, ces dernières sont relativement faibles. En effet, la majorité des décisions de sanctions prises par l'autorité irlandaise ont été invalidées par le Comité européen de la protection des données, jugeant que le montant des amendes était trop faible. À titre d'illustration, lorsque Meta a été condamné à une amende « record » de 390 millions d'euros, le montant estimé par l'autorité irlandaise était dix fois inférieur à celui estimé par le Comité européen : l'écart entre le montant estimé par l'autorité irlandaise et par le CEPD illustre la dépendance économique de la Commission irlandaise face aux géants du numérique, un tel écart ne pouvant pas être pas une simple erreur d'appréciation. Les manquements de la Commission irlandaise remettent en cause l'effectivité du dispositif intégré par le règlement européen.

603. Contrôle de la Cour de Justice. Dans un arrêt du 15 juin 2021, la Cour de justice a rappelé avec fermeté que « le mécanisme de guichet unique ne saurait en aucun cas aboutir à ce qu'une autorité de contrôle nationale, en particulier l'autorité de contrôle chef de file, n'assume pas la responsabilité qui lui incombe en vertu du règlement 2016/679 de contribuer à une protection efficace des personnes physiques contre des atteintes à leurs droits fondamentaux, sous peine d'encourager la pratique d'un *forum shopping*, notamment de la part des responsables de traitement, visant à contourner ces droits fondamentaux et l'application effective [1626] ». Par cet arrêt, la Cour de Justice confirme le lien direct entre l'identification de l'autorité chef de file et le l'effectivité du droit de l'Union européenne[1627] . Surtout, elle rappelle que le système de réparation des compétences « ne doit pas pouvoir être instrumentalisé par les opérateurs économiques qui verraient un effet d'aubaine dans la modération excessive, voire l'inertie, dont pourrait faire preuve une autorité chef de file[1628] ». Ainsi, elle rappelle avec fermeté la répartition des compétences afin d'éviter les détournements du système. Les autorités

[1626] Cour de Justice de l'Union européenne, aff. n° C-645/19, 15 juin 2021, point 68.
[1627] Pouillaude Sibylle, « "Attraper les GAFAM" ou le guichet unique en droit de la protection des données personnelles : fonctionnement, bilan et perspectives », Revue du droit de l'Union européenne, 2023, p. 140.
[1628] Bertrand Brunessen, « La Cour de justice, régulateur de la gouvernance institutionnelle du RGPD », Dalloz Actualité, 30 juin 2021.

de régulation doivent respecter l'obligation de coopération loyale afin de garantir l'effectivité du système : la Cour de justice réaffirme son rôle de gardienne de la cohérence du cadre normatif.

Toutefois, il ressort une certaine impuissance des autorités de contrôle face à la puissance de ces sociétés privées. L'équilibre des pouvoirs est loin d'être une réalité pour le moment.

II. L'impuissance des autorités de contrôle face à la puissance des multinationales

604. Impuissance des autorités de contrôle. Les autorités de contrôle rendent habituellement publiques les sanctions afin de mettre en avant mise en œuvre du cadre normatif. En pratique, le montant des sanctions est modeste au regard à la puissance de ces multinationales (A). Il en ressort une certaine impuissance des autorités de contrôle face aux géants du numérique (B).

A) La puissance des multinationales face aux autorités de contrôle

605. Insuffisance des sanctions. Grâce à l'exploitation des données des utilisateurs, les géants du numérique disposent d'une certaine domination mondiale (1). Afin d'exercer leur pouvoir de sanction au cas par cas, les autorités de contrôle doivent prendre en compte les intérêts privés qui commandent ces acteurs du numérique (2).

1. Une domination publique

606. De plateforme à écosystème. Les services des géants du numérique ont littéralement conquis le monde entier avec leurs services[1629]. Ils ont bénéficié de l'absence de régulation afin d'étendre leur activité à l'échelle du globe[1630] et effectué un réel « coup data » leur conférant un pouvoir sans précédent[1631]. En 2023, les GAFAM ont dégagé plus de 100 milliards de bénéfices

[1629] Le Roy Marylou, « La loyauté des plateformes à l'égard des consommateurs », Thèse, Paris, 2021, p. 303.

[1630] Smyrnaios Nikos, « L'effet GAFAM : stratégies et logiques de l'oligopole de l'internet », Communication & langages, 2016 : « Ils ont également bénéficier de la mondialisation de l'économie : à tel point que pour de nombreux internautes, elles sont internet (Par exemple, en Indonésie, en Thaïlande et aux Philipines, de nombreux répondants à des enquêtes d'usage déclarent utiliser Facebook mais pas internet). », source : Mirani Léo, « Millions of Facebook users have no idea they're using the internet », Quartz, 9 février 2015.

[1631] Basdevant Adrien et Mignard Jean-Pierre, *L'empire des données*, éd. Don Quichotte éditions, 2018, p. 216.

en seulement trois mois[1632]. Les bénéfices de ces entreprises privées leur permettent de poursuivre leurs expansions en développant de nouveaux services et en ayant les capacités de racheter leurs concurrents. En parallèle, de nouveaux acteurs peinent à se développer au regard de la masse de données détenue par ces entreprises. Par exemple, pour la technologie mobilisée au sein du logiciel « ChatGPT », seules des entreprises comme Google peuvent entrainer ces technologies grâce à leur infrastructure et de sa capacité financière[1633]. Ils développent de véritables écosystèmes afin que les utilisateurs utilisent exclusivement leurs services (Google Search, Gmail, Google Maps, etc) : ils sont passés de la plateforme à l'écosystème. Par conséquent, les acteurs du numérique ne cessent de collecter les données dans leur propre écosystème fermé. Ils utilisent des systèmes opaques et inintelligibles de régulation privée leur permettant de collecter toujours davantage de données afin de renforcer leur domination[1634].

607. Domination transnationale. Ils exercent leur domination au niveau transnational, c'est-à-dire un niveau supérieur au niveau international[1635]. Désormais - à côté de la voix des États - les géants du numérique détiennent un certain pouvoir leur permettant de négocier les normes. L'espace transnational est le résultat des activités des entreprises privées ayant déployé leurs services partout dans le monde : « le privé et le public ne sont pas ou ne sont plus compartimentés. Ils sont désormais imbriqués, pour le meilleur et pour le pire, dans tous les

1632 « Astronomique, Meta, Apple, Amazon, Google et Microsoft ont dégagé à eux cinq 100 milliards de dollars de bénéfices en trois mois », La Tribune, publié le 2 février 2024.

1633 Sénéchal Juliette, « L'IA Act déjà obsolète face aux IA de nouvelle génération ? », Dalloz Actualité, 2023 : sur la technologie mobilisée au sein du logiciel ChatGPT « [elle] vise à entraîner en parallèle et simultanément des réseaux de neurones de manière quasi illimitée, décuplant la puissance de calcul en abolissant la frontière de la vitesse d'exécution de certaines tâches, puisqu'elles peuvent être conduites en parallèle. Dès lors, il devient possible de prendre en compte beaucoup plus de données, et de créer des réseaux de neurones moins focalisés sur une tâche spécifique. Profiter de cette innovation n'est cependant possible que pour une entreprise déjà pourvue de très grands centres de calcul, comme Google, déjà dotée de ces centres dédiés à une série d'autres choses, experte dans leur gestion et nantie de la capacité financière suffisante pour investir dans la construction de microprocesseurs dédiés à ce type d'architecture. Tout ceci exclut du marché les plus petites entreprises qui ne peuvent s'offrir cette infrastructure hautement capitalistique. ».

1634 Toledano Joëlle, *GAFA, reprenons le pouvoir,* éd. Odile Jacob, 2020, p. 47.

1635 Sintez Cyril, Le droit construit. Penser le droit par le constructivisme, éd. Dalloz, 2022, p. 69 : « L'international qualifierait ainsi les rapports entre des unités closes sur elles-mêmes et communiquant par l'entremise de représentants ou de mandataires qualifiés ; le transnational qualifierait les échanges partant d'initiatives privées et s'exerçant à travers les frontières des sociétés étatiques. […] Le concept de transnationalité nous invite donc à prêter attention aux phénomènes "internationaux" qui mettent en présence des acteurs non étatiques, et à évaluer la place que ce réseau de relations occupe par rapport à celui qui s'établit entre les États. ».

secteurs de l'activité internationale[1636]. ». Les acteurs du numérique sont devenus incontournables et influencent directement les choix législatifs[1637]. Pire encore, les normes juridiques sont désormais confrontées aux normes numériques. En effet, les géants du numérique produisent en permanence des normes numériques qui peuvent finir par s'imposer comme des standards. Ils créent leurs propres règles en dehors de tout cadre légal[1638] et ils disposent des capacités juridiques et financières pour choisir le meilleur ordre juridique applicable[1639]. Au niveau de la mise en œuvre du droit européen, les géants du numérique ont déjà choisi les États membres les plus attrayants tels que l'Irlande et le Luxembourg.

608. Confusion entre progrès technologique et croissance technologique. Au sein de cet espace numérique, l'effectivité du cadre normatif va dépendre en partie de la volonté des géants du numérique de se soumettre aux normes. Ils ont atteint une hégémonie technologique par le développement de leurs services. Néanmoins, il n'est pas légitime de penser que le monde numérique restera impossible à réguler ou que le législateur est en constant retard sur ces technologies[1640]. Il existe une confusion entre le progrès technologique et la croissance économique : l'extraction et l'exploitation des données des utilisateurs ne sont pas des pratiques inhérentes à l'informatique. Les géants du numérique ont instrumentalisé cette révolution numérique en en faisant leur modèle d'affaires[1641]. Cette confusion leur permet simplement de continuer de mener leurs expériences et de développer des technologies toujours plus

1636 Merle Marcel, *op. cit*., p.231.

1637 Caire Anne-Blandine, *Les nouveaux pouvoirs. Approche pluraliste des foyers de création du droit,* éd. Bruylant, 2017, p. 75 : « La place des multinationales dans la création du droit a incontestablement changé en 30 ans. À l'époque, la création normative des multinationales s'insérait dans le cadre de la lex mercatoria. Le nouveau rôle joué par ces entreprises dans la production normative suit deux voies distinctes et complémentaires, illustration de leur nature "d'unités actives", capables, par leur action propre et dans leur intérêt propre, de modifier leur environnement, y compris normatif. Les entreprises multinationales peuvent intervenir à tous les stades de la régulation publique au moyen de différents procédés de lobbying, de collaboration et de consultation. ».

1638 Kettani Ghizlane, « Quand l'algorithme écrit le droit : les conséquences de la nouvelle normativité numérique », Dalloz IP/IT, 2022, pp. 552-557.

1639 Sintez Cyril, *op. cit.*, p.70.

1640 Basdevant Adrien et Mignard Jean-Pierre, *L'empire des données,* éd. Don Quichotte, 2018, p. 464 : « La vérité est que loi peut tenir le rythme des technologies émergents, tout comme elle s'est montrée capable de le faire avec la médecine, le génie civil, l'agroalimentaire, l'énergie et d'innombrables autres secteurs extrêmement techniques. Les législateurs n'ont pas besoin de comprendre précisément les interactions chimiques d'un nouveau médicament contre le cancer pour créer des processus efficaces d'autorisation de mise sur le marché. […] Pourquoi autorisons-nous les géants du web à mener des expériences humaines à grande échelle, et ce, seulement pour nous rendre compte que ces entreprises sont devenues si puissantes qu'elles en sont ingérables. ».

1641 Zuboff Shoshana et Rose Sean, « Un capitalisme de surveillance », Études, 2021.

performantes afin d'augmenter leurs bénéfices. En effet, il faut prendre en compte les intérêts privés qui régissent les pratiques de ces acteurs.

2. Des intérêts privés

609. Des acteurs privés. Il nous semble nécessaire de cesser de faire confiance à ces acteurs privés : les géants du numérique ne remplissent aucune mission de service public. L'intérêt de ces sociétés cotées en bourse est uniquement de faire des bénéfices afin de satisfaire les actionnaires[1642]. Ainsi, il est important de ne pas adhérer à la parole des dirigeants de ces sociétés. Lorsque Mark Zuckerberg prône que la mission de Facebook est de « connecter les gens, construire la communauté et rassembler le monde », il s'agit d'une imposture[1643]. La mission de Facebook est de collecter les données des utilisateurs afin de maximiser ses revenus. Seulement, proclamer la réelle mission de Facebook risque de provoquer la conscience de certains utilisateurs sur l'usage de leurs données et donc de réduire ses revenus.

Les paroles des dirigeants de ces sociétés sont forcément à tempérer. Tout d'abord, il n'est pas garanti que les successeurs tiendront les promesses des premiers dirigeants[1644]. En réalité, ils semblent eux-mêmes dépassés par leur propre technologie : « quand les dirigeants de la Silicon Valley se justifient en expliquant que l'échelle à laquelle leur plateforme est si gigantesque qu'il est très difficile d'empêcher des tueries de masse d'être diffusées en direct ou de supprimer les appels à un nettoyage ethnique, cela ne peut en aucun cas être accepté comme une excuse, car ils viennent de reconnaître implicitement qu'ils ont créé quelque chose de si grand qu'ils sont devenus incapables de le contrôler[1645] ». Pire encore, lorsque certaines autorités

[1642] Encelot Marjorie, « Les Gafam, ces superpuissances qui peuvent faire dérailler les bourses mondiales », Les échos : « Google, Apple, Facebook, Amazon et Microsoft sont les cinq plus grosses sociétés cotées au monde. Leur valorisation boursière cumulée égale la création de richesse d'un pays du G7 sur un an » ; Leparmentier Arnaud, « Apple et les Gafam, nouvelles valeurs refuge des investisseurs », Le Monde, 4 janvier 2022 : « La firme fondée par Steve Jobs a franchi la barre des 3 000 milliards de dollars de capitalisation boursière. Un record pour un titre désormais considéré comme l'un des actifs les plus sûrs de la planète ».

[1643] Site Facebook, « Mettre les internautes en contact et créer des communautés sur Facebook », sur Facebook Gouvernement, politique et sensibilisation, 4 février 2021 : « La mission de Facebook est de donner à chacun la possibilité de fonder une communauté et de rapprocher les internautes du monde entier. En tant qu'entreprise, nous recherchons les moyens de rapprocher les internautes chaque jour et de leur donner les clés pour aider leurs communautés à grande échelle. ».

[1644] Basdevant Adrien et Mignard Jean-Pierre, *op. cit*. p. 217

[1645] Zuboff Shoshana et Rose Sean, *op. cit*.

sanctionnent les géants du numérique pour non-respect de la vie privée, cela favorise leurs intérêts privés.

610. Des sanctions intéressées. En effet, en 2019 la Federal Trade Commission a sanctionné Facebook par une amende record de cinq milliards de dollars pour absence de protection à la vie privée, suite au scandale de Cambridge Analytica. Néanmoins, la publicité de la sanction a fait augmenter le cours des actions de 3,6%[1646]. Cette augmentation illustre l'impuissance du cadre normatif au regard de la puissance du marché, de leur propre marché des données. De surcroît, le montant de l'amende apparaît démesuré pour tout individu ordinaire. En réalité, le montant est négligeable pour la société Méta puisqu'il s'agit de son chiffre d'affaires réalisé en un mois[1647]. Pire encore, l'accord conclu entre la société et la Commission n'impose pas de limites contraignantes à la collecte de données. Ainsi, Facebook apparaît presque comme bénéfique à la société qui pourra toujours décider de la quantité et des types de données recueillis. L'un des commissaires de la commission estime que cet accord traduit une « immunité totale » pour la société. Malheureusement, il est possible de constater une certaine impuissance des autorités de contrôle face à la domination de ces acteurs privés.

B) L'impuissance des autorités de contrôle face aux géants du numérique

611. Lacunes des actions. Au regard de la puissance des géants du numérique, les autorités de contrôle apparaissent désarmées. Pourtant, le règlement européen pour la protection des données à caractère personnel a renforcé les pouvoirs de ces autorités. En pratique, les autorités de contrôle volontaires manquent de moyens (1). De surcroît, certaines autorités de contrôle apparaissent comme dépendantes des géants du numérique, rendant leurs actions répressives lacunaires (2).

[1646] Wylie Christopher et Blanchard Aurélien, *Mindfuck*, éd. Bernard Grasset, 2020, p. 453 : « Le marché reconnaissant du même coup implicitement, que même la loi ne pouvait mettre un frein à la croissance de ces géants des nouvelles technologies. ».
[1647] Piquard Alexandre, « Facebook : une amende de 5 milliards de dollars et de nouveaux garde-fous, déjà contestés », Le Monde, 24 juillet 2019.

1. Le manque de moyens des autorités de contrôle

612. Le manque de moyens. À l'instar du manque de moyens pour l'application du cadre normatif pour les données publiques, l'autorité de contrôle nationale pour la protection des données à caractère personnel manque de moyens[1648]. Cette lacune pour la Commission nationale de l'informatique et des libertés est une problématique récurrente dans son travail répressif[1649]. Au fil du renforcement de ses nouveaux pouvoirs de sanction, l'autorité n'a pas forcément été dotée des moyens nécessaires. Depuis 1978, la CNIL réclame des moyens adéquats à l'étendue de ses missions. En 2006, l'ancien président de la CNIL réclamait le doublement des moyens humains et financiers au sein de l'organisme[1650]. L'autorité de contrôle n'était pas en mesure de traiter le nombre de dossiers qui lui était soumis. Par conséquent, le manque de moyens entravait le potentiel de cette autorité.

Le manque de personnel ou financier pour l'application des sanctions a toujours été justifié au regard du pouvoir prioritaire de pédagogie dont devait faire preuve l'autorité de contrôle. Néanmoins, il est désormais temps de passer de la pédagogie à la répression. Le droit de la protection des données à caractère personnel existe depuis 1978. Depuis plus de quatre décennies, l'autorité de contrôle fait preuve d'une pédagogie sans faille afin de préparer les organismes à ce changement de paradigme. Désormais, la pédagogie doit être assimilée et les sanctions doivent être effectives : le délai de la mise en conformité est amplement dépassé. En effet, la crédibilité des autorités de contrôle se joue en matière de sanctions[1651].

[1648] Castets-Renard Céline, Favro Karine, « Données à caractère personnel - Collectivités territoriales », Dalloz IP/IT, 2019, « En tout état de cause, pour qu'elles soient efficaces, ces opérations de contrôle sont largement conditionnées par les moyens mis en œuvre par la CNIL. Or, les AAI restant des administrations « légères », même en terme d'effectifs » ; Debet Anne, « Les nouveaux instruments de conformité », Dalloz IP/IT : droit de la propriété intellectuelle et du numérique, N° 12, 2016, p. 592.

[1649] Nana Botchorichvili, « Faut-il réviser le RGPD », Dalloz IP/IT, 2023, 499 : « Tout d'abord, il s'agit selon les constations de la Commission européenne, comme évoqué, de l'absence de ressources suffisantes pour permettre aux autorités de mener à bien leurs missions. En effet, l'écart important entre le nombre considérable et toujours en augmentation du nombre de plaintes, parfois complexes, adressées aux autorités de protection des données, et les ressources inadéquates dont elles disposent en comparaison, ont un impact sur leur capacité d'implication dans les différents mécanismes de coopération, notamment celui du guichet unique, prévu par le RGPD. »

[1650] Brondel Séverine, « La CNIL manque de moyens pour faire face à une tâche de plus en plus lourde », Dalloz actualité, 18 juillet 2007.

[1651] Vergnolle Suzanne, *L'effectivité de la protection des personnes par le droit des données à caractère personnel,* éd. Larcier, 2022, p. 409 ; Desgens-Pasanau Guillaume, « RGPD : entre incertitudes et occasions manquées », Dalloz IP/IT, 2016, p. 335 : « l'équilibre tout entier du règlement européen - et la crédibilité du régulateur - reposent désormais sur les pouvoirs de sanction à posteriori, à charge pour les autorités de

L'entrée en vigueur du règlement européen a renforcé les pouvoirs de sanction de la Commission nationale de l'informatique et des libertés, pourtant l'augmentation du personnel et des moyens n'est toujours pas en adéquation avec le nombre de plaintes des dernières années[1652]. L'autorité de contrôle ne peut exercer effectivement ses pouvoirs de contrôle et de sanctions si elle n'est pas dotée des moyens nécessaires. Dès lors, l'autorité de contrôle doit sélectionner les dossiers et leur éventuelle portée lors de la publication : certains dossiers ne seront pas traités dans les temps et cela a pour conséquence d'affaiblir les pouvoirs des autorités de contrôle. Ainsi, les autorités de contrôle sont confrontées à des difficultés, particulièrement face aux géants du numérique. L'ensemble de ces difficultés menace l'effectivité du droit de l'Union européenne en matière de protection des données à caractère personnel.

2. L'insuffisance des sanctions

613. L'insuffisance des sanctions. Depuis l'entrée en vigueur du règlement européen sur la protection des données à caractère personnel, plus de 4 milliards d'euros de sanctions ont été infligés. Les sanctions ont usuellement fait l'objet d'une publicité afin de mettre en avant le pouvoir répressif dans le cadre du règlement. En réalité, le montant démesuré des sanctions est un « bilan trompe-l'œil », démontrant « une incapacité à contrôler la manière dont les géants du numérique utilisent nos données » déplore NOYB, une association fondée par l'activiste Max Schrems[1653]. À titre d'illustration, l'amende record d'Amazon représente 1,7% du chiffre d'affaires européen du groupe Amazon et 0,3% de son chiffre d'affaires mondial. Finalement, l'amende reportée au chiffre d'affaires semble dérisoire et n'apparaît pas comme une amende effectivement répressive. Les faibles montants ne dissuadent pas les sociétés de réitérer leurs méfaits, d'autant plus que les actes visés permettent d'augmenter considérablement leur chiffre

contrôle de s'en emparer, à défaut de quoi le niveau global de protection des personnes pourrait bien diminuer » ; Gabrié Émile, « Les pouvoirs des autorités de protection des données », Dalloz IP/IT, 2017, p. 268.

[1652] Fagot Vincent, « Face à des missions étendues, la CNIL revendique plus de moyens », Le Monde, 10 avril 2018 : Entre l'inflation du nombre de plaintes et tout le travail entrepris autour du RGPD, se pose la question des moyens. Pour la présidente de la CNIL, dont l'institution est dotée d'un budget de 17 millions d'euros, il s'agit d'un sujet central : « Je le dis maintenant depuis un an : nos moyens sont insuffisants, on a atteint un point de rupture. ». Isabelle Falque-Pierrotin souligne que « là où, dans des pays comparables à la France, nos homologues ont des équipes de 500 personnes, […] nous n'en avons que 200. ».

[1653] Schrems Max, « Le RGPD a une influence parce qu'il est et continuera d'être le standard mondiale », Le Monde, 25 mai 2023 : Le militant autrichien regrette, dans cet entretien, que le RGPD, [qui avait 5 ans lors de l'interview], présente encore des lacunes ; NOYB signifie « None of Your Business », la devise étant « Ma vie privée est None of Your Business ».

d'affaires[1654]. En outre, sur les 4 milliards d'euros infligés dans le cadre du règlement européen, plus de la moitié est cumulée par le groupe Meta. *In fine*, la loi n'est pas appliquée par les géants du numérique car le cadre répressif n'est pas dissuasif pour eux[1655].

[1654] Mohty Ola et Staub Sylvain, « Les sanctions pour violation du RGPD : quelle efficacité ? », Dalloz IP/IT, 2022, pp. 198-203.

[1655] Netter Emmanuel « Le modèle européen de protection des données personnelles à l'heure de la gloire et des périls », *in* Netter Emmanuel (dir.), *Regards sur le nouveau droit des données personnelles*, éd. CEPRISCA, 2019.

614. Conclusion de la section. Les autorités de contrôle disposent d'un rôle cardinal en matière d'effectivité du régime répressif. Le règlement européen renforce leurs pouvoirs afin de réellement sanctionner les manquements à la protection des données à caractère personnel. Les autorités de contrôle disposent d'un panel répressif allant du simple rappel à l'ordre à des sanctions se comptant en millions d'euros.

Pour ce faire, à défaut d'une harmonisation des sanctions pénales, les sanctions administratives font l'objet d'une méthode de calcul individualisée. Afin d'assurer une certaine cohérence des sanctions, plusieurs éléments sont pris en compte comme la nature des données, la durée de la violation ou encore le comportement du responsable de traitement ou du sous-traitant. L'appréciation au cas par cas permet d'individualiser les sanctions au regard de la puissance de l'organisme concerné afin d'assurer une certaine harmonie des sanctions.

Depuis l'entrée en vigueur du règlement européen, le montant des sanctions a été renforcé. L'évolution du montant permet d'assurer l'application de sanctions proportionnée aux manquements et à l'importance de l'organisme. Au niveau national, la CNIL a sanctionné sévèrement plusieurs géants du numérique pour des manquements au droit de la protection des données à caractère personnel. Au niveau européen, il existe également des sanctions similaires.

Pour autant, l'étude approfondie des sanctions démontre une insuffisance du montant au regard de l'importance des organismes. Tout d'abord, le montant des amendes représente généralement une faible part de leur chiffre d'affaires, ce qui entraîne une négligence pour l'application des règles. De surcroît, le mécanisme du guichet unique est générateur de *forum shopping.* La plupart des géants du numérique ont installé leur établissement principal en Irlande en raison du faible régime fiscal. L'installation des géants du numérique en Irlande entraîne une relation de dépendance entre la Commission irlandaise et ces acteurs. Le recours massif aux accords amiables du régulateur irlandais démontre cette dépendance nuisible à l'effectivité du cadre répressif.

Il existe une certaine impuissance du régime répressif face à la puissance des géants du numérique. L'impuissance et le manque de coordination des autorités de contrôle remettent logiquement en cause l'effectivité du régime répressif de la protection des données à caractère personnel.

615. Conclusion du chapitre. L'étude du régime répressif du règlement européen sur la protection des données personnelles fait ressortir la complexité de ce régime. En effet, la transposition du régime de responsabilité classique ne permet pas de se conformer aux règles du numérique. À titre d'illustration, le dommage moral est une notion en construction en matière de protection des données à caractère personnel. L'appréciation de ce dommage fera l'objet d'une jurisprudence abondante afin d'éclaircir l'évaluation de la souffrance morale. Pour autant, l'absence de spécialisation des juges risque de mener une jurisprudence complexe et non harmonisée au sein de l'Union européenne. Il aurait été souhaitable de spécialiser certains juges au sein des tribunaux à l'instar de la propriété intellectuelle.

La complexité du régime répressif est également illustrée par le manque d'actions individuelles en réparation d'une violation du règlement. Malgré la diversité des recours, les personnes concernées n'ont pas forcément conscience de l'exploitation de leurs données à caractère personnel. L'absence de conscience des individus permet aux géants du numérique de perpétuer leurs pratiques illicites. Ainsi, les autorités de contrôle ont leur rôle à jouer afin de protéger les individus contre les pratiques de ces acteurs. Le règlement a renforcé leur pouvoir de sanction afin de mettre en œuvre réellement le cadre normatif.

Néanmoins, les sanctions infligées à ces acteurs restent encore dérisoires au regard de leur puissance. Il est nécessaire de prendre conscience de la domination de ces acteurs privés sur la réglementation des données à caractère personnel. En réalité, ils disposent des moyens afin de respecter la vie privée de leurs utilisateurs. Pour autant, le respect intégral de la réglementation européenne entraînerait la cessation de leurs activités. En effet, le chiffre d'affaires de ces acteurs repose sur la collecte et l'exploitation des données à caractère personnel de leurs utilisateurs. Il sera toujours plus intéressant pour eux de perpétuer leurs pratiques et de payer les amendes plutôt que de respecter la législation. L'exploitation des données à caractère personnel de leurs utilisateurs est nécessaire à leur survie.

616. Conclusion du titre. L'effectivité d'un cadre normatif peut être analysée selon l'acceptation des normes par ses destinataires et par l'application réelle des sanctions. Il s'agit tout d'abord d'apprécier le degré de réalisation des normes dans les pratiques sociales. Le règlement européen sur la protection des données à caractère personnel instaure des droits pour les personnes concernées afin de pouvoir garder le contrôle sur leurs propres données. Les droits des individus doivent être respectés par les responsables de traitement ou les sous-traitants, c'est-à-dire les personnes exploitant ces données. L'effectivité du cadre normatif s'apprécie selon la réalisation pratique des droits et l'application de sanction en cas de non-respect des obligations.

Les individus disposent de nombreux droits grâce au règlement sur la protection des données à caractère personnel. Il peut s'agir de droit personnel ou d'obligations du responsable de traitement de respecter certains principes afin d'exploiter de manière « responsable » les données des utilisateurs. L'étude des droits et obligations fait ressortir une certaine inadéquation de ces droits au regard de l'évolution des technologies. En effet, le principe de minimisation entre en contradiction avec les principes du *Big Data* et le principe de finalité rend incertain l'exploitation secondaire des données. De surcroît, la complexité et l'opacité des traitements limitent la prise de conscience des utilisateurs. L'absence de conscience des utilisateurs face à l'exploitation de leurs données fragilise la notion de consentement. Au final, l'inadéquation des droits au regard de la technologie est un fait délibéré de la part des acteurs du numérique.

Les géants du numérique sont avant tout des acteurs privés agissant pour le compte de sociétés cotées en bourse devant satisfaire des investisseurs. Leurs chiffres d'affaires reposent sur la collecte, l'exploitation et la revente des données à caractère personnel de leurs utilisateurs. Ainsi, ils développent sans cesse des technologies émergentes dans le dessein de manipuler les individus. Les manipulations textuelles ou visuelles ont pour dessein d'obtenir un consentement vide de la part des internautes pour continuer l'exploitation de leurs données. De surcroît, les manipulations permettent de rendre inconscients les utilisateurs sur l'avenir de leurs données.

Malgré une volonté louable de faire respecter la législation, l'étude du cadre répressif sur la protection des données à caractère personnel illustre une effectivité superficielle. Pour le moment, les sanctions n'ont aucun effet dissuasif sur ces acteurs. Il en ressort une certitude : les géants du numérique ont davantage d'intérêt à exploiter les données plutôt que de respecter le cadre européen. L'effectivité limitée de la protection des données à caractère personnel

impacte la cohérence de l'ensemble du cadre normatif, protection censée être le pilier de la construction.

617. Conclusion de la partie. La mise en œuvre du cadre normatif des données est structurée autour de l'articulation des normes et de l'effectivité du cadre. Pour l'articulation des normes, la vision de la pyramide des normes est devenue archaïque. Le monopole de l'État a été substitué par une logique de gouvernance instaurant une multitude d'acteurs pour la mise en œuvre du cadre normatif. Tout d'abord, les groupes sociaux, c'est-à-dire des entreprises privées, participent à l'élaboration et à l'instauration des normes. Par ailleurs, le législateur de l'Union européenne y contribue également et au niveau national, les autorités administratives indépendantes régulent des secteurs techniques.

L'ensemble de ces acteurs sont censés œuvrer de concert afin de garantir une mise en œuvre cohérente du cadre normatif. En réalité, la privatisation des normes par les acteurs du numérique est un danger pour le cadre normatif : ils participent à l'élaboration des normes, s'érigent en régulateur privé et utilisent le code informatique comme source de droit. L'articulation des normes devient artificielle et contrôlée par ces acteurs. L'inintelligibilité de leurs pratiques et leur influence sur l'élaboration et la mise en œuvre du cadre normatif impactent considérablement l'effectivité des normes.

L'effectivité des normes repose tout d'abord sur le respect du droit à la protection des données à caractère personnel, pilier du droit des données. Pourtant, l'étude de la réception des normes par ses destinataires ainsi que l'application réelle des sanctions relève une effectivité superficielle du cadre normatif. Le cadre n'est pas réellement appliqué par les acteurs du numérique, qui profitent de l'évolution des technologies pour contourner les obligations instaurées. Leur chiffre d'affaires repose sur la collecte, l'exploitation et la revente des données à caractère personnel de leurs utilisateurs. Ainsi, ils développent sans cesse des technologies émergentes afin de manipuler les individus et contourner le cadre normatif. Par ailleurs, les sanctions ne sont pas dissuasives pour les acteurs du numérique et inégalement appliquées par les autorités administratives indépendantes. De fait, l'effectivité du cadre normatif est limitée.

CONCLUSION GÉNÉRALE

618. Construction du cadre normatif. Le cadre normatif pour les données se construit depuis plusieurs décennies et s'est considérablement renforcé depuis plusieurs années. Il existe aujourd'hui incontestablement un « droit des données » structuré autour du droit fondamental de la protection des données à caractère personnel. L'ensemble des normes ayant pour objet les données s'est construit et se construit autour du régime de la protection des données à caractère personnel. En réalité, les ambitions de l'Union européenne de construire un cadre normatif cohérent pour les données sont idéalistes pour plusieurs raisons.

619. L'idéalisme d'un équilibre entre des objectifs antinomiques. Tout d'abord, le cadre est structuré autour de deux axes antagonistes : la protection des données à caractère personnel et l'ouverture des données à caractère non personnel. D'une façon idéaliste, l'équilibre aurait dû faire primer la protection des données à caractère personnel au regard de la fondamentalité du régime protecteur. En parallèle, l'ouverture des données par tous les acteurs afin de privilégier les entreprises européennes aurait été l'aboutissement d'une « société parfaite[1656] ». Néanmoins, l'étude du cadre normatif laisse transparaître la volonté récente et prégnante de l'Union européenne de développer l'innovation et l'intelligence artificielle. Pour ce faire, la construction du cadre normatif se poursuit en favorisant l'ouverture des données à caractère non personnel et des données protégées, au détriment de la protection des données à caractère personnel. La cohérence aurait été permise en priorisant les données à caractère personnel et non l'ouverture excessive des données. Le chemin pris par l'Union européenne affaiblit le régime protecteur des données à caractère personnel, affaiblissement amplement cultivé par les acteurs du numérique.

620. L'incompatibilité des influences scabreuses dans la construction d'un cadre normatif. L'étude démontre l'influence des acteurs du numérique dans la construction des normes. Afin d'impacter la cohérence de ce cadre normatif et pérenniser leurs pratiques, les géants du numérique s'infiltrent à chaque étape de la construction du cadre normatif. Lors de l'élaboration des normes, les géants du numérique influencent en amont le contenu des normes afin de promouvoir leurs intérêts et lorsque les campagnes de *lobbying* ne sont pas efficientes,

[1656] Arnaud André-Jean, *Dictionnaire encyclopédique de théorie et de sociologie du droit,* éd. LGDJ, 2018, v° « Idéalisme », sens 2, p. 180.

ils font la promotion de l'autorégulation afin d'établir leurs propres règles, dans leur propre environnement. L'Union européenne se retrouve parfois dépassée par l'inintelligibilité de leurs systèmes et ils en profitent pour développer le droit souple. Lorsqu'ils arrivent à régir leurs pratiques par le droit souple, ils s'avisent par la suite d'intégrer le droit souple dans le droit dur. Par cette technique subreptice, leurs intérêts se retrouvent imprégnés dans les normes de droit dur. La construction d'un cadre normatif protecteur pour les individus ne peut se faire en présence de sociétés privées ayant des intérêts strictement lucratifs reposant sur l'exploitation des données. Les brèches insérées dans les normes peuvent avoir de lourdes conséquences en pratique et vider de substance les principes *a priori* protecteurs pour les individus.

621. Rétablir une responsabilité des acteurs du numérique. Au regard de la puissance de ces acteurs, le droit souple et l'internalisation des normes ne suffisent plus : la confiance octroyée à ces sociétés privées est une vision idéaliste, voire simplement chimérique. Les rapports de pouvoir doivent s'équilibrer et les sociétés privées doivent devenir responsables de leurs technologies, la responsabilisation n'étant plus appropriée à leurs pratiques. Pour le moment, les sanctions demeurent insuffisantes pour réellement impacter leur modèle économique : les sanctions ne sont pas dissuasives pour ces acteurs et l'équilibre des pouvoirs doit être recherché. Factuellement, il est simplement impossible de prendre en compte les intérêts divergents entre l'Union européenne et les géants du numérique tout en garantissant une protection effective des données à caractère personnel.

622. L'incompatibilité des principes protecteurs avec le *Big Data*. Par ailleurs, les technologies émergentes altèrent également le cadre normatif pour les données. Les principes de minimisation ou de finalité deviennent utopiques avec les caractéristiques du *Big Data*. L'intelligence artificielle renforce l'altération de ces principes en évoluant vers des technologies de plus en plus précises, reposant sur de plus en plus de données. L'évolution de ces technologies renverse les dichotomies instaurées entre données à caractère personnel et données à caractère non personnel. Avec le phénomène de *Big Data*, les notions s'entremêlent et se chevauchent, même en cas d'anonymisation des données : les frontières deviennent fragiles et les techniques de réidentification ne cessent de se perfectionner. La porosité est pourtant dangereuse pour les individus et profite aux sociétés privées puisque la distinction entraîne la mise en œuvre de régime fondamentalement opposé.

623. L'exigence de réalisme du cadre normatif existant. En réalité, il n'est pas nécessaire d'aller plus loin dans la construction du cadre normatif. L'ensemble du régime protecteur a été instauré avec le Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données. En revanche, il convient de réaxer les priorités : l'Union européenne doit remettre au centre de sa construction l'Humain et freiner la logique économique. La prévalence des données à caractère personnel ne doit plus être simplement théorique et constituer un obstacle potentiel pour les traitements, elle doit symboliser le pivot de tout traitement.

624. L'instauration de priorités aux secteurs essentiels. En outre, il convient de réaxer la priorité sur le développement de l'intelligence artificielle pour des domaines précis et sélectionnés, tels que la médecine ou l'agriculture. L'environnement est gravement impacté par le développement des technologies émergentes : les technologies numériques consomment énormément d'eau et d'énergie. Malheureusement, l'essor de l'intelligence artificielle ne fait qu'aggraver l'impact environnemental du numérique. Afin de limiter cet impact, il serait donc nécessaire de limiter l'intelligence artificielle aux secteurs essentiels. Par-delà la notion d'altruisme des données, c'est une intelligence artificielle altruiste qu'il convient de développer, c'est-à-dire réaxer l'innovation vers des aspects philanthropiques. Les technologies émergentes peuvent améliorer la condition humaine sur plusieurs aspects, mais il est nécessaire d'identifier en amont ces priorités et de les développer de manière raisonnable. L'amélioration de la condition humaine passe également par l'éducations des individus aux risques du numérique.

625. Les vertus de l'éducation aux risques. En effet, l'individu doit prendre place dans la réalisation du cadre normatif : l'absence de conscience des individus est un obstacle pour l'effectivité du cadre normatif. La vie privée est une notion fondamentale pour les citoyens et pourtant, en l'échange de services gratuits, certains individus sont prêts à abandonner une partie de leur vie privée. Il convient de mettre en place une véritable éducation des individus sur les risques de l'exploitation de leurs données et surtout, au sujet de la manipulation dont ils font l'objet à chaque utilisation de l'environnement numérique. L'éducation doit se faire dès le plus jeune âge en présentant les réseaux sociaux comme un risque et non comme une simple plateforme d'échanges. Il est important, voire primordial, de protéger les mineurs contre les risques à long terme de l'exploitation de leurs données et de les éduquer à l'utilisation raisonnable des réseaux, voire à l'inutilité de ces plateformes.

Le numérique n’est pas dans les nuages et les données ne doivent plus être considérées comme une ressource infinie. L’exploitation des données nécessite une vaste infrastructure physique dommageable pour l’environnement. L’exploitation des données par des sociétés privées représente un risque pour la démocratie, pour le futur des enfants et surtout, pour l’environnement. L’Union européenne doit réaxer sa priorité sur la protection des individus et non sur l’essor de l’intelligence artificielle. Pour le moins, l’intelligence artificielle doit être limitée à certains secteurs bienveillants pour le développement de la société. Les valeurs européennes sont remarquables, à nous de les faire perdurer.

Bibliographie

I. Dictionnaires et encyclopédies

Arnaud André-Jean, *Dictionnaire encyclopédique de théorie et de sociologie du droit*, éd. LGDJ, 2018.

Lamizet Bernard et Silem Ahmed, *Dictionnaire encyclopédique des sciences de l'information et de la communication*, éd. Ellipses, 1998.

Cornu Gérard, *Vocabulaire juridique*, éd. PUF, 2020.

II. Ouvrages

ADFA, *Le temps en droit administratif*, éd. Dalloz, 2022.

Association Henri Capitant des amis de la culture juridique française, *Le droit souple*, éd. Dalloz, 2009.

Barbé Vanessa et Mauclair Stéphanie, *Intelligence artificielle & droits fondamentaux*, éd. Épitoge, 2022.

Barbé Vanessa, *Vers un droit de l'algorithme*, éd. Mare et Martin, 2022.

Barraud Boris ;

- *Repenser la pyramide des normes à l'ère des réseaux*, éd. Harmattan, 2012.
- *Humanisme et intelligence artificielle*, éd. Harmattan, 2022.

Benabou Valérie-Laure et Rochfeld Judith, *À qui profite le clic ?*, éd. Odile Jacob, 2015.

Bensamoun Alexandra, Bertrand Brunessen et Anca Ailincai Mihaela, *Le règlement général sur la protection des données. Aspects institutionnels et matériels*, éd. Mare et Martin, 2020.

Bensamoun Alexandra et Loiseau Grégoire, *Droit de l'intelligence artificielle*, éd. LGDJ, 2022.

Bergé Jean-Sylvestre et Robin Olivier, *Introduction au droit européen*, éd. PUF, 2008.

Bergel Jean-Louis ;

- *Théorie générale du droit*, 4ème édition, éd. Dalloz, 2003.

- *Théorie générale du droit,* éd. Dalloz, 2012.

Bertrand Brunessen ;

- *Les nouveaux modes de production du droit en droit de l'Union européenne : la dialectique du droit institutionnel et du droit matériel*, éd. Presse Universitaire de Rennes, 2018.

- *La politique européenne du numérique,* éd. Bruylant, 2023.

Bertrand Brunessen et Le Floch Guillaume, *La souveraineté numérique*, éd. Bruylant, 2024.

Bévière-Boyer Bénédicte, Dibie Dorothée et Arlotti Clément, *Numérique, droit et société*, éd. Dalloz, 2022.

Bonnet Baptiste et Deumier Pascale, *De l'intérêt de la summa divisio droit public droit privé ?*, éd. Dalloz, 2010.

Bottini Fabien, *Néolibéralisme et américanisation du droit,* éd. Mare et Martin, 2019.

Bouveresse Aude, Ritleng Dominique (dir.), *L'effectivité du droit de l'Union européenne*, éd. Bruylant, 2018.

Braz-Martial Nathalie, *Les mutations de la norme. Le renouvellement des sources du droit*, éd. Economica, 2000.

Bruguière Jean-Michel *et al., Penser le droit de la pensée : mélanges en l'honneur de Michel Vivant*, éd. Dalloz, 2020.

Bruguière Jean-Michel ;

- *La para-propriété intellectuelle*, éd. Dalloz, 2022.

- *L'émergence d'un droit des données*, éd. Dalloz, 2023.

Brun Philippe*, Répertoire de droit civil,* éd. Dalloz, 2023.

Caire Anne-Blandine, *Les nouveaux pouvoirs. Approche pluraliste des foyers de création du droit*, éd. Bruylant, 2017.

Carbonnier Jean ;

- *Sociologie juridique*, éd. PUF, 2004.

- *Droit civil. Les biens*, éd. PUF, 2004.

- *Flexible droit*. *Pour une sociologie du droit sans rigueur,* éd. LGDJ, 2013.

Cassella Sarah, Lasserre Valérie et Lecourt Benoît, *Le droit souple démasqué : articulation des normes privées, publiques et internationales*, éd. Pedone, 2018.

Castets-Renard Céline, *Droit du marché unique numérique et intelligence artificielle,* éd. Bruylant, 2020.

Castets-Renard Céline, Ndior Valère et Rass-Masson Lukas, *Enjeux internationaux des activités numériques : Entre logique territoriale des États et puissance des acteurs privés*, éd. Larcier, 2020.

Castets-Renard Céline et Eynard Jessica, *Un droit de l'intelligence artificielle : entre règles sectorielles et régime général : perspectives comparées*, éd. Bruylant, 2023.

Chamoux Jean-Pierre, *L'appropriation de l'information*, éd. Librairies techniques, 1986.

Chénédé François, Lequette Yves, Simler Philipe, Terré François, *Droit des obligations*, éd. Dalloz, 2022.

Clam Jean et Martin Gilles, *Les transformations de la régulation juridique*, éd. LGDJ, 1998.

Couret Alain, *Un juriste pluriel*, éd. Dalloz, 2020.

De Streel Alexandre et Jacquemin Hervé, *Intelligence artificielle et droit,* éd. Larcier, 2017.

De Terwangne Cécile, Degrave Elise, Queck Robert et Dusollier Séverine, *Law, norms and freedoms in cyberspace. Droit, normes et libertés dans le cybermonde. Liber amicorum Yves Poullet*, éd. Larcier, 2018.

De Terwangne Cécile et Rosier Karen, *Le règlement général sur la protection des données. Analyse approfondie,* éd. Larcier, 2018.

Delmas-Marty Mireille ;

- *Pour un droit commun*, éd. Le Seuil, 1994.

- *Le Pluralisme ordonné. Les forces imaginantes du droit (II),* éd. Le Seuil, 2006.

- *La refondation des pouvoirs. Les forces imaginantes du droit (III)*, éd. Le Seuil, 2009.

Demogue René, *Les notions fondamentales du droit privé ; essai critique pour servir d'introduction à l'étude des obligations*, éd. Dalloz, 1911.

Derave Charly, Frydman Benoît et Genicot Nathan, *L'intelligence artificielle face à l'État de droit*, éd. Bruylant, 2024.

Douville Thibault, *Droit des données à caractère personnel*, éd. LGDJ, 2023.

Dubouis Louis et Gueydan Claude, *Les grands textes du droit de l'Union européenne*, éd. Dalloz, 8ème édition, 2010.

Eckert Gabriel et Kovar Philippe, *L'interrégulation*, éd. L'Harmattan, 2017

Émeric Nicolas, *Penser les flux normatifs*, éd. Mare et Martin, 2018.

Eynard Jessica ;

- *Les données personnelles. Quelle définition pour un régime de protection efficace ?*, éd. Michalon, 2013.

- *L'identité numérique*, éd. Larcier, 2020.

Eynard Jessica et Macilotti Giorgia, *L'identité numérique en construction. Quels enjeux et quels modèles ?,* éd. Bruylant, 2024.

Fabre Magnan Muriel, *Droit des obligations, 2, Responsabilité civile et quasi-contrats,* éd. PUF 2021.

Favro Karine ;

- *Droit de la régulation des communications numériques,* éd. LGDJ, 2018.

- *Communications numériques : régulation et résolution des litiges*, éd. LGDJ, 2019.

Féral-Schuhl Christiane, *Cyberdroit,* 8ème édition, éd. Dalloz, 2021.

Frison-Roche Marie-Anne ;

- *Les risques de la régulation*, éd. Dalloz, 2005.

- *Internet, espace d'interrégulation*, éd. Dalloz, 2016.

- *Régulation, Supervision, Compliance,* éd. Dalloz, 2017.

- *Les outils de la compliance*, éd. Dalloz, 2021.

- *Les buts monumentaux de la compliance*, éd. Dalloz, 2022.

- *La juridictionnalisation de la compliance*, éd. Dalloz, 2023.

G'Sell Florence, *Le Big Data et le Droit*, éd. Dalloz, 2020.

Gaudrat Philippe et Sardain Frédéric, *Traité de droit civil du numérique. Tome 1, Droit des biens,* éd. Larcier, 2015.

Gény François, *Science et technique en droit privé positif*, éd. Sirey, 1921.

Girard Charlotte, *Des droits fondamentaux au fondement du droit,* éd. Éditions de la Sorbonne, 2010.

Hachez Isabelle, Cartuyvels Yves et Dumont Hugues, *Les sources du droit revisitées. Théorie des sources du droit*, éd. Presses universitaires Saint-Louis Bruxelles, 2012.

Jestaz Philippe, *Mélanges en l'honneur de Philippe Jestaz. Libres propos sur les sources du droit,* éd. Dalloz, 2006.

Jestaz Philippe, *« Sources du droit, sources de droit : une cartographie »,* éd. Dalloz, 2022.

Kelsen Hans, *Théorie pure du droit*, éd. LGDJ, 1999.

Lajoie André, Janda Richard et Rocher Guy, *Théories et émergence du droit : pluralisme, surdétermination et effectivité,* éd. Bruylant, 1998.

Lambert Dominique, *La robotique et l'intelligence artificielle*, éd. Lessius, 2019.

Lapousterle Jean, *L'influence des groupes de pression sur l'élaboration des normes,* éd. Dalloz, 2009.

Lasserre Valérie, *Le nouvel ordre juridique. Le droit de la gouvernance*, éd. LexisNexis, 2015.

Latil Arnaud, *Le droit du numérique. Une approche par les risques*, éd. Dalloz, 2023.

Le Goff Joan et Onnée Stéphane, *Puissances de la norme. Défis juridiques et managériaux des systèmes normatifs contemporains,* éd. EMS Éditions, 2017.

Le Goffic Caroline, Pailler Ludovic et Grynbaum Luc, *Droit des activités numériques*, éd. Dalloz, 2023.

Lequette Suzanne, *Droit du numérique*, éd. LGDJ, 2024.

Lombard Martine, *Droit et économie de la régulation. Règles et pouvoirs dans les systèmes de régulation*, éd. Presses de Sciences Po, 2004.

Malabat Valérie et Zabalza Alexandre, *La propriété au 21ème siècle, un modèle ancestral toujours adapté aux grands enjeux de notre environnement ?*, éd. Dalloz, 2021.

Martial-Braz Nathalie, Rochfeld Judith, *Droit des données personnelles. Les spécificités du droit français au regard du RGPD,* éd. Dalloz, 2019.

Martine Behar-Touchais, Martial-Braz Nathalie et Riffard Jean-Francois, *Les mutations de la Norme : Renouvellement des sources du droit,* éd. Economica, 2011.

Martucci Francesco, *Droit de l'Union européenne*, 2ème édition, éd. Dalloz, 2019.

Mekki Mustapha, *La force et l'influence normatives des groupes d'intérêt*, éd. Lextenso, 2011.

Molfessis Nicolas, *Quel avenir pour la responsabilité civile ?,* éd. Dalloz, 2015.

Mongoin David, *Philosophie du droit*, éd. Dalloz, 2022.

Monville Claire, *Variations sur le droit de la société de l'information*, éd. Bruylant, 2002.

Netter Emmanuel ;

- *Les biens numériques,* éd. CEPRISCA, 2015.

- *Numérique et grandes notions de droit privé,* éd. CEPRISCA, 2019.

- *Regards sur le nouveau droit des données personnelles*, éd. CEPRISCA, 2019.

Nevejans Nathalie, *Données et technologies numériques. Approche juridique, scientifique et éthique*, éd. Mare et Martin, 2021.

Olson Terry et Cassia Paul, *Le droit international, le droit européen et la hiérarchie des normes,* éd. PUF, 2006.

Oppetit Bruno, *Philosophie du droit*, éd. Dalloz, 2022.

Ost Francois, Van de Kerchove Michel ;

- *Le système juridique entre ordre et désordre,* éd. PUF, 1988.

- *De la pyramide au réseau ? Pour une théorie dialectique du droit,* éd. FUSL, 2022.

Parat Hélène, Angelergues Jacques, Cointot Françoise, *Mémoires : se souvenir, oublier*, éd. Presses Universitaires de France, 2021.

Peyrou-Bartoll Sylvie, *Nouvelles technologies et droit européen : quel droit face à la disruption numérique ?,* éd. Mare et Martin, 2022.

Poullet Yves, *Le RGPD aux défis de l'intelligence artificielle*, éd. Larcier, 2020

René Savatier, *Traité de la responsabilité civile en droit français*, éd. LGDJ, 2016.

Ripert Georges, *Les forces créatrices du droit*, éd. LGDJ, 1955.

Rochfled Judith, *Les grandes notions du droit privé*, éd. PUF, 2022.

Sève René, *Philosophie et théorie du droit*, éd. Dalloz, 2016.

Sintez Cyril, *Le droit construit. Penser le droit par le constructivisme*, éd. Dalloz, 2022.

Sirinelli Pierre, Azzi Tristan, Bensamoun Alexandra etc, *Mélanges en l'honneur de Pierre Sirinelli,* éd. Dalloz, 2022.

Terré François, Simler Philippe, Lequette Yves, *Droit civil. Les obligations*, éd. Dalloz, 2018.

Terré François et Molfessis Nicolas ;

- *Introduction générale au droit,* éd. Dalloz, 2020.

- *Introduction générale au droit*, éd. Dalloz, 2022.

Thibierge Catherine, *Densification normative. Découverte d'un processus*, éd. Mare et Martin, 2014.

Thibierge Catherine, *La force normative. Naissance d'un concept*, éd. LGDJ, 2009.

Vergnolle Suzanne, L*'effectivité de la protection des personnes par le droit des données à caractère personnel,* éd. Larcier, 2022.

III. Ouvrages non juridiques

Abiteboul Serge, *Sciences des données : de la logique du premier ordre à la Toile*, éd. Fayard : Collège de France, 2012.

Abiteboul Serge et Cattan Jean, *Nous sommes les réseaux sociaux,* éd. Odile Jacob, 2022.

Babinet Gilles et Orsenna Erik, *Big Data, penser l'homme et le monde autrement,* éd. Le Passeur, 2015.

Basdevant Adrien et Mignard Jean-Pierre, *L'empire des données*, éd. Don Quichotte, 2018.

Bourdin Aymeric, *Le numérique : locomotive de la 3e révolution industrielle ?,* éd. Ellipses, 2013.

Brasseur Christophe, *Enjeux et usages du big data,* éd. Lavoisier, 2016.

Broudoux Evelyne et Chartron Ghislaine, *Big data, Open data. Quelles valeurs ? Quels enjeux ?,* éd. de Boeck, 2014.

Cardon Dominique, *À quoi rêvent les algorithmes*, éd. Seuil, 2015.

Cattaruzza Amaël, *Géopolitique des données numériques : Pouvoir et conflits à l'heure du Big Data*, éd. Le Cavalier Bleu, 2019.

Chignard Simon et Benyayer Louis-David, *Datanomics*, éd. FYP, 2015.

Chignard Simon, *Open data*, éd. FYP, 2012.

Cointot Jean-Charles, Eychenne Yves, *La révolution du Big Data : Les données au cœur de la transformation de l'entreprise*, éd. Dunod, 2014.

Colin Nicolas et Verdier Henri, *L'Âge de la multitude,* éd. Armand Colin, 2012.

Davadie Philippe et Kempf Olivier, *La donnée n'est pas donnée*, éd. Kawa, 2016.

Delort Pierre, *Le Big Data*, éd. PUF, 2018.

Douglas Edwards*, I'm Feeling Lucky : The Confessions of Google Employee Number*, éd. Allen Lane, 2011.

Dugain Marc, Labbé Christophe, *L'homme nu. La dictature invisible du numérique*, éd. Robert Laffon, 2016.

Haugen Frances, *La vérité sur Facebook,* éd. Fayard, 2024.

Mayer-Schönberger Viktor et Cukier Kenneth, *Big Data. A Revolution that will transform how we live, work and think,* éd. Houghton Mifflin Harcourt, 2013.

Meyer Vincent, *Transition digitale*, éd. LEH, 2017.

Laborit Henri, *L'esprit du grenier*, éd. Grasset, 1992.

Lejeune Yannick, *Big, fast, open data : Décrire, décrypter et prédire le monde : l'avènement des données*, éd. FYP, 2014.

Pariser Eli, *The filtre Bubble*, éd. Penguin Group, 2012.

Pascual Frank, *Black box society. Les algorithmes secrets qui contrôlent l'économie et l'information*, éd. FYP, 2015.

Patino Bruno ;

- *La civilisation du poisson rouge,* éd. Grasset, 2020.

- *Tempête dans le bocal*, éd. Grasset, 2022.

- *Submersion,* éd. Grasset, 2023.

Pitron Guillaume, *L'enfer numérique : Voyage au bout d'un Like,* éd. Les Liens qui Libèrent, 2021.

Toledano Joëlle, *GAFA : Reprenons le pouvoir*, éd. Odile Jacob, 2020.

Wylie Christopher et Blanchard Aurélien, *Mindfuck. Le complot Cambridge Analytica pour s'emparer de nos cerveaux*, éd. Bernard Grasset, 2020.

Zuboff Soshana, *The Age of Surveillance Capitalism : The Fight for a Human Future at the New Frontier of Power*, éd. Profile Books, 2018.

IV. Articles de revues juridiques

Acquisti Alessandro et Rochelandet Fabrice, « Les comportements de vie privée face au commerce électronique », La Découverte, 2011.

Ancel Bruno, « L'intelligence artificielle au XXIe siècle : outil juridique fiable ou amplificateur d'injustices ? », LPA, 31 mai 2024.

Ancel Marie-Elodie, « À propos de la "marge de manœuvre" laissée par le règlement général sur la protection des données aux États membres de l'Union européenne », Revue critique de droit international privé, n° 3, Dalloz, 2019.

Anciaux Arnaud et Farchy Joëlle, « Données personnelles et droit de propriété », Revue internationale de droit économique, 2015.

Andrieu Bernard, « Traquer son bien-être et propriété des données : quel droit des sportifs 3.0 sur leur corps vivant ? », JS, 2016, n° 162.

Auby Jean-Bernard, « Les défis auxquels sont confrontés nos droits administratifs », RFDA, 2024, 241.

Autin Jean-Louis, « Le devenir des autorités administratives indépendantes », RFDA, 2010, 875.

Barra Vincent, « Apprentissage automatique et réseaux de neurones », Tangente, hors-série n° 68, octobre 2018.

Barraud Boris, « Les nouveaux défis de la recherche sur les sources du droit », Revue de la Recherche Juridique, Droit prospectif, 2017, 164.

Barron Andrew et Voss Gregory, « La culture et son impact sur les actions politiques des entreprises », Revue française de gestion, 252, Lavoisier, 2015.

Beauchesne Bénédicte « La dépendance européenne et nationale face aux nouveaux acteurs du numérique », Dalloz IP/IT, 2021, 125.

Beguin-Faynel Céline ;

- « Objets connectés et appréciation du risque », Responsabilité civile et assurances, n° 3, mars 2023, dossier 10.

- « Assurances et nouvelles technologies - Objets connectés et appréciation du risque », Responsabilité civile et assurances, n°3, mars 2023.

Benabou Valérie-Laure ;

- « Entrée par effraction d'une notion juridique nouvelle et polymorphe : le contenu numérique », Dalloz IP/IT, 2017.

- « L'extension du domaine de la donnée », Legicom, n° 59, Victoires éditions, 2017.

- « Une cinquième liberté de circulation numérique ? Est-ce possible ? Est-ce utile ? », RTD eur., 2021, 287.

- « La Cour de justice, gardienne d'une "souveraineté européenne" sur les données », RAE, 2018/1.

Bénel Aurélien, « 15 ans de Web 2.0 : Imitation pop ou extension du domaine de l'Hypermédia ? », Hypertextes et hypermédias, produits, outils et méthodes, 2019.

Benezech Ludovic, « Les actes de droit souple des autorités administratives, vers l'affermissement d'une portée normative », RFDA, 2024, 467.

Bensamoun Alexandra et Zolynski Célia, « Big data et privacy : comment concilier nouveaux modèles d'affaires et droits des utilisateurs ? », LPA, 2014.

Bensoussan Alexandra « À terme, le droit de valoriser ses propres données apparaît inéluctable », RLDI, 2018.

Bensamoun Alexandra et Masmi-Dazi Fayrouze, « Intelligence artificielle : pour l'émergence d'un écosystème européen éthique et compétitif », La semaine juridique, n° 3, 22 janvier 2024.

Bensamoun Alexandra et Loiseau Grégoire, « L'intelligence artificielle à la mode éthique », D., 2017, n° 24, 1371.

Bensamoun Alexandra et Loiseau Grégoire, « L'intelligence artificielle : faut-il légiférer ? », D., 2017, 581.

Bensamoun Alexandra et Zolynski Célia, « Cloud computing et big data », La Découverte, 2015.

Benzerafa-Alilat Manel et Gibert Patrick, « De l'inflation normative à l'amplification des lois dans le processus parlementaire », Revue française d'administration publique, 182, Institut national du service public, 2022.

Bérard-Quélin Bernard, « La naissance d'un droit voisin au profit des éditeurs et agences de presse », Légipresse, 2019, 107.

Berezkina Ekaterina, « Cookies : la CNIL précise les obligations de contrôle de conformité entre responsables de traitement conjoints », Dalloz IP/IT, 2023.

Bergé Jean-Sylvestre, « La sphère des données et le droit : nouvel espace, nouveaux rapports aux territoires », Journal du droit international, octobre 2016, n°4.

Bergé Jean-Sylvestre et Le Métayer Daniel, « Phénomènes de masse et droit des données », CCE, 2018.

Berlin Dominique, « Les retombées inattendues de l'affaire Snowden », La Semaine Juridique, n° 42, octobre 2015, 1107.

Bernard Meyer Hippolyte, « La question de la lutte contre les contenus haineux dans le cyberespace, une réponse nécessairement européenne ? », Revue de l'Union européenne, 2024.

Bernheim Emmanuelle, « Le "pluralisme normatif" », Revue interdisciplinaire d'études juridiques, 67, Université Saint-Louis - Bruxelles, 2011.

Bertrand Brunessen ;

- « La volonté de réguler les activités numériques », RTD eur., 2021, 160.

- « La souveraineté numérique européenne : une "pensée en acte" ? », RTD eur., n° 249, 2021.

- « La Cour de justice, régulateur de la gouvernance institutionnelle du RGPD », Dalloz actualité, 30 juin 2021.

- « Les enjeux de la surveillance numérique », RTD eur., 2021, 175.

- « La gouvernance des données dans la régulation européenne de l'intelligence artificielle », RTD eur., 2022, n° 315.

- « La lutte contre la diffusion des contenus à caractère terroriste en ligne », RTD eur., 2022, 485.

Besse Philippe, Castets-Renard Céline, Garivier Aurélien, « L'IA du Quotidien peut-elle être Éthique ? », Loyauté des Algorithmes d'Apprentissage Automatique, 2018.

Betty Jeulin, « Amendement de l'Artificial Intelligence Act : la théorie confrontée à la pratique », Dalloz Actualité, 14 juin 2023.

Bleusez Marion, « La réception du droit souple par le contentieux de droit privé », Dalloz, Justice et Cassation, 2023, 119.

Bigot Christophe, « Dispositif actuel de lutte contre la haine en ligne », Chapitre 1 : Les discours de haine, une catégorie en construction, Pratique du droit de la presse, Dalloz, 2023/2024.

Boillet Nicolas, Baranes Edmond, Sauron Jean-Luc, « Le règne des données », Cahiers français, 2021.

Boizard Maryline, « Le consentement à l'exploitation des données à caractère personnel : une douce illusion ? », CCE, n°3, étude 6, 2016.

Bordais Pierre, « L'autodétermination informationnelle à l'épreuve des évolutions technologiques », Dalloz IP/IT, 2024.

Bore Louis, « L'action en représentation conjointe : class action française ou action mort-née ? », Dalloz, 1995, 267.

Botchorichvili Nana ;

- « Bilan des sanctions prononcées par les autorités européennes de protection des données : quelles tendances ? », CCE, n° 3, mars 2024.
- « Faut-il réviser le RGPD ? », Dalloz IP/IT, 2023.

Bougeard Aurélien, « Les dispositions relatives à l'accès et au portage des données : code de bonne conduite et bonnes pratiques », Dalloz IP/IT, 2020, 408.

Boul Maxime, « Réflexions sur la notion de donnée publique », Revue française d'administration publique, n° 167, École nationale d'administration, 2018.

Boullier Valentin, « CNIL et Microsoft : délibération du 11 mai 2023 clôturant l'injonction faite par la CNIL à Microsoft le 19 décembre 2022 en matière de cookies », Dalloz Actualité, 16 juin 2023.

Bourgeault Guy, « L'éthique et le droit aujourd'hui : quand les fondations sont ébranlées... », Les cahiers de droit, 34.

Bourgeois Matthieu et Moine Marion, « Articulation entre le RGPD et la loi informatique et libertés : le réveil des nations ? », Cahier législatif nº 280, 2018.

Bourgeois Matthieu et Thibierge Louis, « Droit de la donnée : plaidoyer pour un régime général », La semaine juridique, n° 20, 2020.

Boy Laurence, « Réflexions sur le droit de la régulation », D., 2001, 3031.

Breteau Lise, « Numérique et environnement : émergence d'un sujet majeur », CCE, n° 12, décembre, 2023, étude 24.

Brisson Jean-François, « La diversité des régulateurs nationaux sectoriels », RFDA, 2014, 869.

Brondel Séverine, « La CNIL manque de moyens pour faire face à une tâche de plus en plus lourde », Dalloz actualité, 18 juillet 2007.

Brousseau Éric, « Régulation de l'Internet », Revue économique, 52, Presses de Sciences Po, 2001.

Calvès Anne-Emmanuèle, « Empowerment », Revue Tiers Monde, 200, Armand Colin, 2009.

Camus Aurélien, « La propriété des données publiques », Revue française d'administration publique, n° 167, 2018.

Cassar Bertrand, « Gouvernance des données », Répertoire IP/IT et Communication, Dalloz, 2022.

Cassar Bertrand, « L'importance de la gouvernance des données dans l'usage de systèmes d'IA générative », Dalloz IP/IT, 2023, p. 513.

Cassar Bertrand, Plédel Chloé et Galbois-Lehalle Diane, « L'articulation du projet de règlement sur l'intelligence artificielle avec le droit du numérique européen », Dalloz IP/IT, 17 juillet 2023.

Castets-Renard Céline ;

- « Les opportunités et risques pour les utilisateurs dans l'ouverture des données de santé », RLDI, n° spécial 108, 2014.

- « Invalidation du Safe Harbor par la CJUE : tempête sur la protection des données personnelles aux États-Unis », D., 2016, 88.

- « Adoption du Privacy Shield : des raisons de douter de la solidité de cet accord », Dalloz IP/IT, 2016, 444.

- « Brève analyse du règlement général relatif à la protection des données personnelles », Dalloz IP/IT, 2016.

- « Quels lien établir entre les USA et l'UE en matière de vie privée et protection des données personnelles ? », Dalloz IP/IT, 2016

- « Comment construire une intelligence artificielle responsable et inclusive ? », Recueil Dalloz, 2020.
- « Quelle politique européenne de l'intelligence artificielle ? », RTD eur., n° 297, 2021.

Catala Pierre, « Ébauche d'une théorie juridique de l'information », D., 1984.

Chagny Muriel, « La régulation des plateformes numérique par le droit de la concurrence », Revue Lamy de la concurrence, n° 129, 1er juillet 2023.

Chardeaux Marie-Alice, « Réseaux sociaux et données personnelles : avons-nous pris la mesure des menaces qui nous guettent ? », CCE, n° 1, janvier 2021.

Charrier Benjamin, « Le consentement exprimé par les mineurs en ligne », Dalloz IP/IT, 2018, 333.

Chemain Régis, « La relation juridique des GAFA avec l'Union européenne », Rev. UE, 2023, 90.

Chevallier Jacques, « La gouvernance, un nouveau paradigme étatique ? », Revue française d'administration publique, 105-106, Institut national du service public, 2003.

Chevallier Jacques et Cluzel-Métayer Lucie, « Introduction », Revue française d'administration publique, n° 167, École nationale d'administration, 2018.

Chevallier Jacques ;
- « Vers l'État-plateforme ? », Revue française d'administration publique, n° 167, École nationale d'administration, 2018.
- « Autorités administratives indépendantes et État de droit », Civitas Europa, vol. 37, n° 2, 2016.
- « Le statut des autorités administratives indépendantes : harmonisation ou diversification ? », RFDA, 2010, 896.

Chopin Frédérique, « Responsabilité pénale des fournisseurs de contenu », Répertoire IP/IT et Communication, Dalloz, 2024.

Cluzel-Métayer Lucie ;

- « Les limites de l'open data », AJDA, 2016.

- « La loi pour une République numérique : l'écosystème de la donnée saisi par le droit », AJDA, 2017.

- « La construction d'un service public de la donnée », Revue française d'administration publique, 2018, 167.

- « Contrôler les contenus ? », Pouvoirs, 185, Le Seuil, 2023.

Coglianese Cary, « Regulating Machine Learning : The Challenge of Heterogeneity », Competition Policy International : TechReg Chronicle, 2023, Public Law Research Paper.

Cohen Dany, « Ampleur et qualités du consentement donné par clic de souris », LPA, n°164, 18 août 2014.

Colpas Anna, « L'approche européenne de l'Intelligence Artificielle : brève analyse de l'interaction avec le droit à la vie privée et à la protection des données à caractère personnel », L'observateur de Bruxelles, 2021/4, n° 126.

Coupez François, Péronne Géraldine, « Consentement aux cookies : quelle est la bonne recette ? », Dalloz IP/IT, 2020, 189.

Crichton Cécile ;

- « Cookies : sanction de Google par la CNIL confirmée », Dalloz IP/IT 2022, 62.

- « Données personnelles et cases pré-cochées : toujours un défaut de consentement », Dalloz Actualité, 1 décembre 2020.

- « Transfert de données vers les USA : l'arrêt Schrems II », 22 juillet 2020, Dalloz actualité.

Danis-Fatôme Anne ;

- « Quelles actions judiciaires en cas de violation du RGPD ? », CCE, avril 2018.

- « Cookies et autres traceurs : Articulation des sources, compétence de la CNIL et manquements aux règles applicables aux traceurs à des fins publicitaires », CCE, 2021.

- « Open data - Quels garde-fous pour le partage des données ? », CCE, n° 5, mai 2022, 37.

Daragon Elise, « Étude sur le statut juridique de l'information », D., 1998, chron., p. 64.

De Montecler Marie-Christine, « Les lignes directrices de la CNIL sur les cookies partiellement censurées », AJDA, 2020, 1264.

Debet Anne ;

- « Les nouveaux instruments de conformité », Dalloz IP/IT : droit de la propriété intellectuelle et du numérique, n° 12, 2016, 592.

- « Quand les jouets nous espionnent », CCE, 2018.

- « Le consentement dans le Règlement Général sur la Protection des données : rôle et définition », CCE, n° spécial avril 2018, étude n° 9.

- « La CJUE étend, une nouvelle fois, le champ d'application du RGPD », CCE, n° 1, janvier 2023, 5.

- « Faut-il réviser la loi informatique et libertés ? », Dalloz IP/IT, 2023, 505.

Debet Anne et Martial-Braz Nathalie « Les sources du droit de la protection des données en question », Dalloz IP/IT, 2023.

Debet Anne, « La CJUE et le préjudice moral issu d'une violation de données », CCE, n° 2, février 2024.

Debiès Élise, « Big data de santé et autodétermination informationnelle », Revue française d'administration publique, n° 167, 2018.

Deltorn Jean-Marc, « La protection des données personnelles face aux algorithmes prédictifs », Revue des droits et libertés fondamentaux, 2017.

Desgens-Pasanau Guillaume ;

- « RGPD : entre incertitudes et occasions manquées », Dalloz IP/IT, 2016, 335.

- « L'articulation des ordres juridiques européen et national à travers l'exemple du règlement général sur la protection des données personnelles », Cahier législatif, 2018.

- « Nouveau règlement européen sur les données. Quelles conséquences pour les professionnels ? Morceaux choisis et premiers éléments d'analyse », Communication commerce électronique, avril 2024.

Desmarais Pierre, « La réforme de l'open data suppose une approche globale », La Semaine Juridique Edition Générale, 2014.

Deumier Pascale ;

- « Reconnaissance du lobbying en France », RTD civ., 2010.

- « Quand le droit souple rencontre le juge dur », RTD civ., 2016, 571.

Dormont Sarah, « L'élaboration de la norme en droit d'auteur : les discours sur la légitimité », Légipresse, 2019, 79.

Douville Thibault ;

- « Les dangers de la collecte des données de santé par les tiers intéressés (gafam, assureurs…) », Journal du Droit de la Santé et de l'Assurance, n° 20, 2018.

- « La responsabilité des responsables du traitement et des sous-traitants à l'égard des personnes concernées : une grande oubliée », RAE, 2021, p. 29.

Douville Thibault et Netter Emmanuel, « Présentation critique du Data governance act », RTD com. 2022. 561.

Douville Thibault, « Règlement sur les marchés numériques (digital markets act) : questions choisies sur son champ d'application après la désignation des premiers contrôleurs d'accès », RTD com., 2023, 873.

Douville Thibault, « De l'approche extensive de la prise de décision exclusivement automatisée », D., 2024, 1000.

Dubois Lorette, « Une nouvelle pierre à l'édifice de la notion de donnée à caractère personnel », Dalloz Actualité, 1er juin 2023.

Dubois Lorette et Gaullier Florence, « Publicité ciblée en ligne, protection des données à caractère personnel et ePrivacy : un ménage à trois délicat », Legicom, n° 59, 2017.

Eckhoudt Marjorie, « Propos introductifs », Revue internationale de droit économique : Les grandes entreprises échappent-elles au droit ?, Association internationale de droit économique, 2016.

Emeric Nicolas et Matthieu Robineau, « Prendre le droit souple au sérieux ? À propos de l'étude annuelle du Conseil d'État pour 2013 », La semaine juridique, n° 43, 2013.

Eréséo Nicolas, « Libre circulation des données et droit de la concurrence (à propos du règlement du 14 novembre 2018 relatif à la libre circulation des données non personnelles) », Dalloz IP/IT, 2020, 414.

Eynard Jessica, « RGPD "empouvoirement" individuel : promesse tenue ou espoir déçu ? », RAE, 2021.

Falque-Pierrotin Isabelle, « La CNIL face à l'économie de la donnée », D., 2015, 2432.

Farchy Joëlle et Tallec Steven, « De l'information aux industries culturelles, l'hypothèse chahutée de la bulle de filtre », Questions de communication, Éditions de l'Université de Lorraine, 2023.

Farchy Joëlle et Denis Juliette, « La culture des données », Presse des mines, 2020.

Favro Karine et Zolynski Célia, « De la régulation des contenus haineux à la régulation des contenus (illicites) », Légipresse, 2019, 461.

Favro Karine ;

- « Introduction », Légicom, 56, 2016.
- « La démarche de compliance ou la mise en œuvre d'une approche inversée », Legicom, n° 59, 2017
- « La CNIL, une autorité à "l'âge de la maturité" », Dalloz IP/IT, 2018.
- « "Les données non personnelles" : un nouvel objet juridique », Dalloz IP/IT, 2020.

Favro Karine et Zolynski Célia, « DSA, DMA, l'Europe encore au milieu du gué », Dalloz IP/IT, 2021, 217.

Favro Karine, « Transformation numérique de l'administration », Répertoire de service publique, Dalloz, avril 2023.

Féral-Schuhl Christiane et Sinibaldi Justine, « Le RGPD challengé par l'intelligence artificielle », L'observateur de Bruxelles, 2023/2, n° 132.

Foucart Romain, « Acte fondateur ou coup d'épée dans l'eau ? Observations relatives à la stratégie européenne pour les données », Revue de l'Union européenne, n° 647.

Fourcade Marion, « La mouche et le traqueur : alignement et désaxement dans le capitalisme au XXIe siècle », Regards croisés sur l'économie.

Frayssinet Jean, « La régulation du respect de la loi Informatique, fichiers et libertés par le droit pénal », Légicom, n° 42, Victoires éditions, 2009.

Fricero Natalie, « Algorithmes et nouvelle génération de droits humains. À propos de la Charte éthique européenne d'utilisation de l'intelligence artificielle dans les systèmes judiciaires et leur environnement », JCP, 2018, 1331.

G'Sell Florence ;

- « Les réseaux sociaux ou la privatisation de l'espace informationnel en ligne », Revue de droit international d'Assas, n°5, mai 2022, 5.

- « Le Conseil de surveillance de Facebook et l'affaire Trump. Les limites du concept de "tribunal d'entreprise" », La Semaine Juridique Edition Générale, n° 22, 31 mai 2021.

Gabrié Émile, « Les pouvoirs des autorités de protection des données », Dalloz IP/IT, 2017, p. 268

Gaudemet Yves, « La régulation économique ou la dilution des normes », RDP, 2017.

Gaye-Palettes Matthieu, « Entre justice privée et justice étatique », Pouvoirs, 178, septembre 2021, 21.

Geffrey Edouard, « Droits fondamentaux et innovation : quelle régulation à l'ère numérique ? », Les nouveaux cahiers du Conseil Constitutionnel, n ° 52.

Gola Romain, « Le règlement européen sur les données personnelles, une opportunité pour les entreprises au-delà de la contrainte de conformité », Légicom, 2017, 29.

Goldman Berthold, Frontières du droit et lex mercatoria, Archives de philosophie du droit, 1964.

Gossa Julien, « Les données non personnelles : un tech checking », Dalloz IP/IT, 2020.

Griguer Merav, Schwart Julie, « RGPD et loi Informatique et Libertés modifiée. Une harmonie en demi-teinte », Revue Internationale de la Compliance et de l'Éthique des Affaires n° 03, 2018.

Grange Maryline, « Internet rattrapé par le droit », Politique étrangère, Institut français des relations internationales, 2019.

Groffe-Charrier Julie, « La loi est-elle dictée par le code ? », Dalloz IP/IT, 2020.

Gufflet Myriam, « Les efforts des autorités nationales et du Comité européen de la protection des données pour une application efficace du RGPD », l'Observateur de Bruxelles, n° 132, 2023/2.

Guichardaz Rémy et Pénin Julien, « L'économie de la réutilisation des données (non personnelles) », Dalloz IP/IT, 2020, p. 218.

Guinard Dorian, « À propos du soft law en droit de l'Union européenne : analyses théorique et pratique », Rev. UE 2013, 609.

Haas Gégard et Astier Stéphane, « Les biais de l'intelligence artificielle : quels enjeux juridiques ? », Dalloz IP/IT, 2019.

Haquet Arnaud, « Le pouvoir réglementaire des autorités administratives indépendantes », RDP, 2008.

Hardouin-Ayrinhac Marie-Lou, « Cookies publicitaires », La lettre juridique, 2 février 2022.

Hoang Mathilde, « Les données publiques : qu'en est-il de leur ouverture et de leur réutilisation ? », Cahiers Français, 2021.

Huttner Liane ;

- « Mesurer l'effectivité du RGPD », RAE, n° 2023/4.

- « Décisions automatisées : le réveil d'un géant endormi ? », CCE, n° 2, février 2024, étude 3.

Idot Laurence ;

- « Données personnelles - DMA, DSA, DGA, DA ou les dernières avancées du marché des services numériques », Europe n° 8-9, Août-septembre 2022.

- « Une nouvelle étape dans la réalisation du marché unique des données », Europe, n° 8-9, août-septembre 2023

Idoux Pascale, « Régulateurs nationaux et régulateurs européens », Revue du droit public, n°2, 2014.

Iliopoulou-Penot Anastasia, « La Constitution numérique européenne », RFDA, 2023, 945 .

Jestaz Philippe, « L'erreur "fondamentale" de Kelsen », RTD civ, 2023.

Jeulin Betty, « Amendement de l'Artificial Intelligence Act : la théorie confrontée à la pratique », Dalloz Actualité, 14 juin 2023.

Jommi Adel, « Le RGPD : un atout ou un frein pour la cybersécurité ? », Dalloz IP/IT, 2019.

Joubert Natalie, « La dernière pierre (provisoire ?) à l'édifice du droit international privé européen en matière familiale », Revue critique de droit international privé, Dalloz, 2017.

Keller Jonathan, « Le Data Act : de nouvelles règles de partage des données », Dalloz Actualité, 20 décembre 2023.

Kettani Ghizlane « Quand l'algorithme écrit le droit : les conséquences de la nouvelle normativité numérique », Dalloz IP/IT, 2022, 552.

Knetsch Jonas, « La désintégration du préjudice moral », Recueil Dalloz, 2015, 443.

Knetsch Jonas, « Les actions civiles en réparation fondées sur une violation du RGPD : Vers un nouveau contentieux de masse ? », La Semaine Juridique Edition Générale, publié le 26 septembre 2022.

Koops Bert-Jaap, « The Trouble with European Data Protection Law », International Data Privacy Law, 8 October 2014.

Lacombe César, « Pour une approche spatiale du numérique : repenser le design numérique », Management des technologies organisationnelles, 2021.

Laneret Nathalie, Knittel Rachel Baudequin Anne, « Protection des données à caractère personnel : quand le droit de la concurrence s'en mêle », Dossier IP/IT, 2017.

Laneret Nathalie, « L'accountability et la protection effective des données personnelles dans un monde digital connecté », RUE, n° 634, 2020.

Lanna Maximilien ;

- « Les objets connectés : entre remise en question de la notion de vie privée et évolution du droit des traitements des données personnelles », Revue de droit public n°5, 2017.

- « Données publiques et protection des données personnelles », Revue française d'administration publique, n° 167, École nationale d'administration, 2018.

Lassègue Jean, « Que faut-il entendre par "surveillance" en contexte digital ? », Revue pratique de la prospective et de l'innovation, n° 2, dossier 16, novembre 2021.

Lasserre Capdeville Jérôme, « Nouvel éclaircissement de la notion de données personnelles », Dalloz IP/IT, 2023.

Lasserre-Kiesow Valérie, « L'ordre des sources ou le renouvellement des sources du droit », D., 2006, 2279.

Lebeau Marianna Denise et Balducci Alexandre, « Adoption des lignes directrices modificatives de la CNIL relatives aux cookies et traceurs à la suite de la décision du Conseil d'État du 19 juin 2020 : quelles conséquences en pratique ? », Dalloz IP/IT, 2021, 41.

Legeais Dominique, « Scoring. Encadrement de la technique du score par la Commission nationale de l'informatique et des libertés », RTD com., 2007, 208.

Leroy Yann, « La notion d'effectivité du droit », Droit et société, n° 79, Éditions juridiques associées, 2011.

Loubere Nicholas, « L'âge d'or de l'algorithme : le crédit social et la financiarisation de la gouvernance en Chine », Action publique. Recherche et pratiques, 3, Institut de la gestion publique et du développement économique (IGPDE), 2019.

Louvaris Antoine ;

- « Régulation économique et inflation normative », RDP, 2014, 304.
- « Droits fondamentaux et innovation : quelle régulation à l'ère numérique ? », Les nouveaux cahiers du Conseil constitutionnel, n° 52.
- « Le droit souple a trouvé ses juges : un foisonnement régulé », Justice et Cassation, 2023, 191.

Magnon Xavier, « L'ontologie du droit », Revue française de droit constitutionnel, 120, Presses Universitaires de France, 2019.

Maisnier-Boché Lorraine, « Le défi de l'amélioration des droits des parties dans le cadre des procédures de contrôle et de sanction », CCE, n° 4, avril 2024.

Malinvaud Philippe, « Lobbying et construction », RDI, 2012, 361.

Mallet-Poujol Nathalie ;

- « Plateformes en ligne et modération des contenus : la liberté d'expression à l'épreuve du concept d'évidence », Légipresse, 2024, 348.
- « Appropriation de l'information : l'éternelle chimère », Recueil Dalloz, 1997, 38.

Manokha Ivan, « Le scandale Cambridge Analytica contextualisé », Cultures Conflits, n° 109, 2018.

Marchal Aurélie, « Réflexions sur l'innovation organisationnelle à l'ère du numérique », éd. EMS, n° 7, septembre 2014.

Mariez Jean-Sébastien et Godfrin Laura, « Censure de la loi "Avia" par le Conseil constitutionnel : un fil rouge pour les législateurs français et européens ? », Dalloz Actualité, 29 juin 2020.

Martial-Braz Nathalie, Rochfeld Judith, Gattone Emilie, « Quel avenir pour la protection des données à caractère personnel en Europe ? Les enjeux de l'élaboration chaotique du règlement relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données », Dalloz, 2013.

Martial-Braz Nathalie ;

- « Le renforcement des droits de la personne concernée », Dalloz IP/IT, 2017, 253.
- « L'abus de textes peut-il nuire à l'efficacité du droit ? », Dalloz IP/IT, 2018.
- « Le droit au déréférencement : vraie reconnaissance et faux-semblants », Dalloz IP/IT, 2019, 631.
- « Quant Meta se voit contraint d'abandonner la publicité ciblée sans consentement », CCE, n° 12, décembre 2023.
- « Deux Acts pour une stratégie numérique ! », CCE, n° 9, septembre 2023.
- « Fumée blanche sur le front des transferts des données, really ? », CCE, n° 10, octobre 2023, 9.
- « Meta sous tension : tirs croisés de régulation numérique ! », CCE, n° 12, décembre 2023.
- « Souveraineté numérique en danger ! », CCE, n°5, mai 2024.
- « La loi SREN : un texte de plus au millefeuille numérique, so frenchy ! », CCE, n° 7, Juillet-août 2024.

Masson Florent, « Quel modèle "propriétaire" pour les données personnelles ? », RTD civ, octobre 2022.

Mattatia Fabrice, « Pour en finir avec le mythe du consentement RGPD », JCP, n° 16, 2020.

Maxwell Winston, « Données publiques et données personnelles : un “mariage pour tous” aux limites de la légalité », 22 juillet 2013, édition Multimédia, n° 84.

Maxwell Winston et Taïeb Sarah, « L’accountability, symbole d’une influence américaine sur le règlement européen des données personnelles ? », Dalloz IP/IT, 2016, 123.

Merabet Samir ;

- « Le Digital Service Act : permanence des acteurs, renouvellement des qualifications », La Semaine Juridique Edition Générale n° 41, 17 octobre 2022, 1175.

- « Droit et Intelligence artificielle - Chronique », La Semaine Juridique, édition générale n° 25, juin 2024.

Metallinos Nathalie ;

- « La protection des données au service de l’émancipation du consommateur », CCE, 2017, 17.

- « Lignes directrices du G29 sur le consentement », CCE, 2019.

- « L’évolution du droit européen en matière de protection des données à caractère personnel », L'observatoire de Bruxelles, n° 93, 2013.

Michaël Ghnassia, « Après la censure de la loi contre la haine en ligne, quel avenir pour la répression des contenus haineux sur internet ? », Légipresse, 2020, 419.

Mohty Ola et Staub Sylvain, « Les sanctions pour violation du RGPD : quelle efficacité ? », Dalloz IP/IT, 2022.

Molfessis Nicolas, « La loi de la course », RTD civ. 1998. 778

Monnerie Nils, « Les défis de la commercialisation des données après le RGPD : aspects concurrentiels d'un marché en développement », Revue internationale de droit économique, 2018.

Moreau Defarges Philippe, « Gouvernance. Une mutation du pouvoir ? », Le Débat, n° 115, 2001.

Moreau Michel, « Sur un droit obèse », Revue de jurisprudence commerciale, n° 3, 267.

Mouchette Julien, « Haro sur les obligations de localisation des données non personnelles », Dalloz IP/IT, 2020.

Moussier Paul, « Les conséquences pour les personnes publiques du Data Governance Act », Revue internationale de droit des données et du numérique, 2023.

Moutot Romain, « Lutte contre les pratiques déloyales des GAFAM : le DMA est publié ! », Dalloz Actualité, 16 novembre 2022.

Musson Margot, « Loi SREN : renforcement des pouvoirs de l'ARCOM et de la CNIL au service de la protection des internautes », Dalloz IP/IT, 17 juin 2024.

Naftalski Fabrice, « Le nouveau cadre de protection des données Union européenne-États-Unis, portée et limites », Dalloz IP/IT, 2023, 600.

Narayanan Arvind et Felten Edward, « No silver bullet: De-identification still doesn't work », White Paper, 2014.

Ndior Valère, « Le Conseil de surveillance de Facebook, "service après-vente" de la liberté d'expression ? », D., 2020, 1474.

Ndior Valère, « Le Conseil de surveillance de Facebook et la protection des libertés », RDLF, n°23, 2022.

Netter Emmanuel ;

- « L'identité numérique », Droit et numérique, 2019.

- « Sanction à 50 millions d'euros : au-delà de Google, la CNIL s'attaque aux politiques de confidentialité obscures et aux consentements creux », Dalloz IP/IT, 2019, 165.

- « À quoi sert le principe de transparence en droit des données personnelles ? », Dalloz IP/IT, novembre 2020, 611.

- « La portabilité, un droit à inventer », Dalloz IP/IT, 2020, 352.

- « « Refuser tous les cookies ». Espoirs et mirages d'une régulation par les boutons », Dalloz IP/IT 2022, 392.

- « L'instauration d'une procédure simplifiée de sanction au profit de la CNIL », RTD com, 2022.

- « Du simple au décuple. Hésitations autour de la juste proportion des sanctions en droit des données personnelles : le cas Accor », RTD com., 2022, 575.

- « La publicité ciblée n'est pas « nécessaire » au contrat de réseau social. Le crépuscule d'un modèle d'affaires », RTD com., 2023, 359.

- « Quand la force de conviction du scoring bancaire provoque sa chute. L'interprétation extensive, par la CJUE, de la prohibition des décisions entièrement automatisées », RTD com., 2024, 342.

- « Le choix de la sanction en droit des données à caractère personnel », CCE, n° 3, mars 2024.

- « "Payer ou consentir" n'est généralement pas une alternative acceptable. Un clou de plus dans le cercueil de la publicité ciblée », RTD com., 2024.

Ochoa Nicolas, « Pour en finir avec l'idée d'un droit de propriété sur ses données personnelles : ce que cache véritablement le principe de libre disposition », RDFA, 2015.

Osman Filali, « Avis, directives, codes de bonne conduite, recommandations, déontologie, éthique, etc. : réflexion sur la dégradation des sources privées du droit », RTD civ., 1995, 509.

Padova Yann, « l'IA Act est-il réconciliable avec le RGPD et comment ? », Revue Lamy Droit de l'Immatériel, n° 209, 2023.

Pailhès Bertrand, « Comment définir et réguler les « données d'intérêt général » ? », Annales des Mines, 2018.

Pailler Ludovic ;

- « Quelle réparation pour le préjudice moral du fait d'une violation du droit de la protection des données ? », Dalloz Actualité, 2022.

- « La Cour de justice de l'Union européenne, pompier pyromane malgré elle : l'articulation des voies de recours ouvertes à la personne concernée par un traitement de données à caractère personnel », Légipresse, 2023.

Paquet Philippe, « De l'information à la connaissance », Cahier de recherche, 2006.

Pascal Alix, « Il est plus facile pour un chameau de passer par le chas d'une aiguille que pour les responsables de traitement d'obtenir un consentement libre et éclairé au dépôt et à la lecture de cookies tiers », Légipresse, 2020, 495.

Pascual Alexandre, Guéguen Nicolas, « La technique du « vous êtes libre de… » : induction d'un sentiment de liberté et soumission à une requête ou le paradoxe d'une liberté manipulatrice », Revue internationale de psychologie sociale, 2002.

Passa Jérôme, « La propriété de l'information : un malentendu ? », Droit & Patrimoine, 2001, n° 91.

Pauliat Hélène, « La contribution du droit souple au désordre normatif », RDP, 2017.

Paulin Boris, « La restitution des données : difficultés pratiques », Dalloz IP/IT, 2017, 33.

Pellegrini François, « La portabilité des données et des services », Revue française d'administration publique (RFAP), n° 167, École nationale d'administration, 2018.

Perray Romain et Uzan-Naulin Julie, « Existe-t-il encore des données non personnelles ? », Dalloz IP/IT, 2017.

Perray Romain et Favreau Julie, « Data Governance Act : le cerbère de la réutilisation des donneés ? », Communication, Commerce électronique, n° 3, Mars 2023.

Perray Romain ;

- « Data Act : une loi pour mieux distribuer la manne des données », LexisNexis, Revue trimestrielle, 2024.

- « Droits des personnes concernées. Droit à ne pas faire l'objet d'une décision automatisée », JurisClasseur Communication, 2024.

Perriault Jacques, « Traces numériques personnelles, incertitude et lien social », La Revue, 53, CNRS Éditions, 2009.

Petel Antoine, « Quel bilan normatif pour l'Europe numérique ? », LexisNexis, Europe, n°5, mai 2024.

Petel Antoine, « L'Acte sur la gouvernance des données. L'Union européenne dévoile le premier pilier du marché européen des données », La Semaine juridique. Édition générale, 2022.

Peugeot Valérie, « Données personnelles : sortir des injonctions contradictoires », VECAM, 13 avril 2014.

Pineau Karl et Fabre Aurelia, « Évaluer la captologie et le design persuasif des services numériques. Approche empirique de mesure de la persuasion et proposition d'une matrice d'évaluation », Information, données & documents, 2021.

Piwnica Emmanuel, « La dévolution d'un pouvoir de sanction aux autorités administratives indépendantes », RFDA, 2010, 915.

Pons Ronan et Risser Laurent, « Biais et discriminations dans les systèmes d'intelligence artificielle », Dalloz IP/IT, 2022.

Potel-Saville Marie, « Dark Patterns : l'étau législatif se resserre (enfin ?) sur les interfaces manipulatrices ou trompeuses », Revue pratique de la prospective et de l'innovation (RPPI), 2022, dossier 19.

Pouillaude Sibylle, « "Attraper les GAFAM" ou le guichet unique en droit de la protection des données personnelles : fonctionnement, bilan et perspectives. », Revue des affaires européennes, n° 2023/1.

Poullet Yves ;

- « Consent : "The privacy bug" », La confiance numérique, travaux de la Chaire sur la confiance numérique, Paris.

- « Cinq ans après - le RGPD est-il toujours la solution ? », R.D.T.I., n° 90, 2023.

- « Cinq ans après : le RGPD et les défis du profilage à l'heure de l'intelligence artificielle », Revue des affaires européennes, Numéro 1, 2021.

- « "La troisième voie", une voie difficile. Quelques réflexions autour de la politique européenne en matière d'intelligence artificielle », Revue Lamy Droit de l'Immatériel, n° 182, 1er juin 2021.

Pouzet Clémentine, « Le droit aux prises des incertitudes de l'intelligence artificielle », 20èmes Rencontres des Jeunes Chercheurs en Intelligence Artificielle, Juin 2022, Saint-Etienne, France.

Prevost Jean-Baptiste, « La fabrique des données : à propos du codage numérique du droit et de ses limites », Gazette du Palais, 22 janvier 2019, n° 3.

Pucheral Philippe, Rallet Alain, Rochelandet Fabrice, Zolynski Célia, « La Privacy by design : une fausse bonne solution aux problèmes de protection des données personnelles soulevés par l'Open data et les objets connectés ? », Legicom, n° 56, Victoires éditions, 2016.

Puig Pascal, « Hiérarchie des normes : du système au principe », RTD civ., 2001.

Raymond Martin, « Le droit en branches », D., 2002, 1703.

Rebillard Franck et Smyrnaios Nikos, « Les infomédiaires, au cœur de la filière de l'information en ligne », Réseaux, La Découverte, 2010.

Renondin de Hauteclocque Stanislas, « L'intelligence artificielle : les différents chemins de la régulation », Éthique publique. Revue internationale d'éthique sociétale et gouvernementale, 2021.

Revet Thierry « La propriété de la personnalité », Gazette du Palais, 2007, n° 139.

Ripert Georges, « Le prix de la douleur », D., 1948.

Rochfeld Judith, « Données à caractère personnel. Données des mineurs », Répertoire IP/IT et Communication, Juillet 2019.

Rochfeld Judith, « L'encadrement des décisions prises par algorithme », Dalloz IP/IT, 2018, 474.

Rochfeld Judith et Zolynski Célia « Quelles limites aux traitements des émotions ? », Dalloz IP/IT, décembre 2023.

Roda Christophe, « Le Digital Markets Act (2e partie). Contraindre les contrôleurs d'accès », Communication commerce électronique, n° 3, Mars 2023.

Rouvroy Antoinette et Berns Thomas, « Gouvernementalité algorithmique et perspectives d'émancipation », La Découverte, 2013.

Rouvroy Antoinette ;

- « Le droit à l'autodétermination informationnelle et la valeur du développement personnel : une réévaluation de l'importance du droit à la protection de la vie privée pour la démocratie », État de droit et virtualité, Thémis, Montréal.
- « Des données sans personne : le fétichisme de la donnée à caractère personnel à l'épreuve de l'idéologie des Big Data », 2014.

Saillant Clara ;

- « Articulation du RGPD et du DGA : l'analyse économique de la CNIL », Dalloz Actualité, 13 mars 2023.
- « Les recours prévus par le RGPD peuvent être exercés simultanément et de manière indépendante », Dalloz Actualité, 25 janvier 2023.
- « Modération en ligne à la demande de la police londonienne : le Conseil de surveillance de Meta s'improvise régulateur et juge », Dalloz Actualité, 15 décembre 2022.

Sauron Jean-Luc et Quéméner Myriam, « Le régime de sanction du RGPD : quand la complétude l'emporte sur la cohérence », Dalloz IP/IT, 2018.

Schwartz Julie et Schlich Rémy, « Loi SREN : de nouveaux pouvoirs pour la CNIL », Cahiers de droit de l'entreprise n° 3, Mai-Juin 2024.

Ségur Philippe, « Le terrorisme et les libertés sur l'internet », AJDA, 2015, 160.

Sénéchal Juliette ;

- « Vote des parlementaires européens sur l'AI Act : vers une réglementation accrue des IA, des modèles de fondation et des IA génératives, s'inspirant du DSA, du Data Act et du RGPD ? », Dalloz Actualité, 22 juin 2023.

- « L'IA Act déjà obsolète face aux IA de nouvelle génération ? », Dalloz Actualité, 1er février 2023.

Sirinelli Pierre et Prévost Stéphane, « Les maîtres de la GAFAXIE », Dalloz IP/IT, 2019, 10, 525.

Smyrnaios Nikos, « L'effet GAFAM : stratégies et logiques de l'oligopole de l'internet », Communication & langages, 188, 2016.

Solove Daniel, « Introduction : Privacy Self-Management and the Consent Dilemma », 2013, Harvard Law Review.

Tanghe Hélène et Gibert Paul-Olivier, « L'enjeu de l'anonymisation à l'heure du big data », Revue francaise des affaires sociales, 2017.

Teller Marina, « Vers l'acceptabilité sociale des algorithmes ou comment passer de l'"algocratie" à la démocratie algorithmique », Revue pratique de la prospective et de l'innovation, n°1, 2022.

Temple Henri, « Le droit de la consommation est-il subversif ? », Études de droit de la consommation, Dalloz, 2004, 1067.

Teresi Laurent, « L'open data et le droit de l'Union européenne », AJDA, 2016, 87.

Thibierge Catherine, « Le droit souple. Réflexion sur les textures du droit », RTD civ., 2003.

Thieulin Benoît, « Gouverner à l'heure de la révolution des pouvoirs », Pouvoirs, 164, 2018.

Thuillas Olivier et Wiart Louis, « Plates-formes culturelles : quelles alternatives aux géants du numérique ? », Nectart, n° 8, Éditions de l'Attribut, 2019.

Tinière Romain, « L'apport de la Charte des droits fondamentaux à la protection des données personnelles dans l'Union européenne », RAE, n° 2018/1.

Toledano Joëlle, « La Commission européenne, la norme et sa puissance », Pouvoirs, 185, Le Seuil, 2023.

Tran Christophe, « La CNIL dans l'environnement européen de la protection des données personnelles : renouveau d'une autorité administrative indépendante », Droit Administratif n°1, Janvier 2022, étude 1.

Türk Pauline, « L'autodétermination informationnelle, un droit fondamental émergent ? », Dalloz IP/IT, 2020, n° 11, 616.

Vallée Laurent, « Élaboration de la norme et influence », Justice et Cassation, 2012.

Vandenhende Elodie, « Application du DMA par les autorités de concurrence et le juge de droit commun », Revue Lamy de la concurrence, n° 129, 1er juillet 2023.

Vanderlinden Jacques, « Contribution en forme de mascaret à une théorie des sources du droit au départ d'une source délicieuse », RTD civ., 1995, 69.

Vandevelde Maya, « La violation du RGPD ne suffit pas à ouvrir droit à réparation : il faut aussi prouver un préjudice », Dalloz, 5 juin 2023.

Verdier Henri et Vergnolle Suzanne, « L'État et la politique d'ouverture en France », AJDA, 2016.

Viangalli Francois, « Le concept de données en droit du numérique. Essai de définition. », Revue Droit de de l'Immatériel, n° 202, 1er avril 2023.

Vivant Michel ;

- « La privatisation de l'information par la propriété intellectuelle », Revue internationale de droit économique, 2006.

- « Les exceptions nouvelles au lendemain de la loi du 1er août 2006 », D., 2006.

Warusfel Bertrand, « Régulation du numérique et souveraineté dans le cyberespace », Dalloz IP/IT, 2022.

Ziller Jacques, « L'interrégulation dans le contexte de l'intégration européenne et de la mondialisation », Revue française d'administration publique, 109, Institut national du service public, 2004.

Zolynski Célia et Le Roy Marylou, « La portabilité des données personnelles et non personnelles, ou comment penser une stratégie européenne de la donnée », Légicom, Revue du droit de la communication des entreprises et de la communication publique, 2017, 105.

Zolynski Célia, « Big data : pour une éthique des données », Information, données & documents, 2015.

Zolynski Célia, Le Roy Marylou et Levin François, « L'économie de l'attention saisie par le droit », Dalloz IP/IT 2019, 614.

Zolynski Célia ;

- « Un nouveau droit de propriété intellectuelle pour valoriser les données : le miroir aux alouettes ? », Dalloz IP/IT, 2018, 94.

- « Les nouveaux contours de l'action de groupe et de l'action collective au lendemain de la loi pour la protection des données : un empowerment renforcé », Dalloz IP/IT, 2018.

- « Contrats de fourniture de contenus et de services numériques. À propos de la directive (UE) 2019/770/UE du 20 mai 2019 », La Semaine Juridique Édition Générale, n° 47, 18 novembre 2019, 1181.

- « La place du règlement (UE) 2018/1807 dans la construction du droit des données de l'Union européenne », Dalloz IP/IT, 2020, 429.

Zolynski Célia et Maxwell Winston, « Protection des données personnelles », Recueil Dalloz, 2020, n° 22.

Zorn Caroline, « Le jeu de données composites : données personnelles et (en même temps) non personnelles ? », Dalloz IP/IT, 2020.

Zuboff Shoshana et Rose Sean, « Un capitalisme de surveillance », Études, 2021.

V. Thèses

Bougeard Aurélien, « Le phénomène de Big Data et le Droit, Pour une appréhension juridique par sa décomposition technique », Thèse, Strasbourg, 2022.

Christina Koumpli, « Les données personnelles sensibles : contribution à l'évolution du droit fondamental à la protection des données personnelles : étude comparée : Union Européenne, Allemagne, France, Grèce, Royaume-Uni », Thèse, Paris, 2019.

Dejean-Ozanne Christophe, « Économie de la donnée et plateforme en ligne », Thèse, Toulouse 1, 2019.

Chloé Dornbierer, « Les choses non rivales : essai sur le régime juridique de l'information », Thèse, Aix-en-Provence, 2022.

Lanna Maximilien, « La protection des données à caractère personnel à l'épreuve de l'automesure connectée », Thèse, Paris, 2019.

Laroche Benjamin. « Le big data à l'épreuve du règlement européen sur la protection des données », Thèse, Toulouse, 2020, p. 158.

Le Roy Marylou « La loyauté des plateformes à l'égard des consommateurs », Thèse, Paris, 2021.

Lesaulnier Frédérique, « L'information nominative », Thèse, Paris, 2005.

Macrez Franck, « Créations informatiques : Bouleversement des droits de propriété intellectuelle ? », Thèse, Montpellier, 2007.

Merabet Samir, *Vers un droit de l'intelligence artificielle,* éd. Dalloz, 2020, p. 48.

Vergnolle Suzanne, L*'effectivité de la protection des personnes par le droit des données à caractère personnel,* éd. Larcier, 2022.

VI. Rapports, études, communiqués et avis

ARCOM, « Lignes directrices prises pour contribuer à la lutte contre la dissémination des contenus haineux en ligne », 2022.

Association française des Correspondants à la protection des données à caractère personnel (AFCDP), « Quantified Self connecté et Informatique & Libertés », novembre 2015, version 10.3 finale.

Aureau Tristan, Cytermann Laurent, Duchesne Claudine, Morel Mathieu, Vachey Laurent, « Rapport relatif aux données d'intérêt général », Rapport d'étape, septembre 2015.

Benabou Valérie-Laure et Zolynski Célia, « Rapport sur les données et contenus numériques », CSPLA, 2018.

Bessot David, Billard Pierre, Bourgeois Matthieu *et al*., « L'empreinte de la donnée sur le vivant : Essai pour un numérique responsable », étude, 2024.

Borthorel Eric, « Rapport sur la politique publique de la donnée, des algorithmes et des codes sources », 2020.

Braun Gilles, Aristide Cavaillès Jean, Moulet Jean Marc *et al*., « Données numériques à caractère personnel au sein de l'éducation nationale », Rapport n° 2018-016, février 2018.

CEPD ;

- « Guidelines 05/2020 on consent under Regulation 2016/679 », 4 mai 2020.
- « Lignes directrices sur les interfaces truquées dans les interfaces des plateformes de médias sociaux », 2022.
- « Report ont Cookie Banner Task Force », 17 janvier 2023.

- « Lignes directrices 04/2022 sur le calcul des amendes administratives », version 2.1, adoptées le mardi 24 mai 2023.

CNnum ;

- « Neutralité des plateformes : réunir les conditions d'un environnement numérique ouvert et soutenable », Rapport, Conseil National du Numérique, Paris, mai 2014.

- « La libre circulation des données dans l'Union Européenne », Avis, avril 2017.

- « La levée des obligations de localisation des données », Avis sur la libre circulation des données en Europe, 2017.

Comité économique social et environnemental (CESE), « Impacts de l'intelligence artificielle : risques et opportunités pour l'environnement », Avis, 24 septembre 2024.

Commission européenne ;

- « La Commission propose une réforme globale des règles en matière de protection des données pour accroître la maîtrise que les utilisateurs ont sur leurs données, et réduire les coûts grevant les entreprises », Communiqué de presse, IP/12/46, 25 janvier 2012.

- « Stratégie pour un marché unique numérique en Europe », COM(2015) 192 final.

- « Créer une économie européenne fondée sur les données », Communication de la commission au parlement européen, au conseil, au comité économique et social européen et au comité des régions, COM(2017) 9 final.

- « Le pacte vert pour l'Europe », COM(2019) 640 final, 11 décembre 2019.

- « Lignes directrices relatives au règlement concernant un cadre applicable au libre flux des données à caractère non personnel dans l'Union européenne », COM (2019) 250 final.

- « Lignes directrices en matière d'éthique pour une intelligence artificielle digne de confiance », avril 2019.

- « Intelligence artificielle. Une approche axée sur l'excellence et la confiance », Livre blanc, Bruxelles, 19 février 2020, COM(2020),

- « Façonner l'avenir numérique de l'Europe », Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions, COM(2020) 67 final.
- « Une stratégie européenne pour les données », Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions, COM(2020) 66 final.
- « Impact assessment report accompanying the DGA proposal », Rapport, SWD(2020), 295 final.
- « Services numériques : La Commission désigne le premier ensemble de très grandes plateformes en ligne et de moteurs de recherche », Communiqué de presse, 25 avril 2023.
- « La Commission désigne une deuxième série de très grandes plateformes en ligne au titre du règlement sur les services numériques », Communiqué de presse, 20 décembre 2023.
- « La Commission désigne Shein en tant que très grande plateforme en ligne, au titre du règlement sur les services numériques », Communiqué de presse, 28 avril 2024.
- « Législation sur l'intelligence artificielle (IA) : le Conseil donne son feu vert définitif aux premières règles mondiales en matière d'intelligence artificielle », Communiqué de presse, 21 mai 2024.

Commission nationale de l'informatique et des libertés ;

- « Informatique et libertés », Guide, édition 2010.
- « Le corps, nouvel objet connecté. Du quantified self à la M-Santé : les nouveaux territoires de la mise en données du monde », Cahiers IP, n° 02, mai 2014.
- « Comment permettre à l'homme de garder la main ? Les enjeux éthiques des algorithmes et de l'intelligence artificielle », rapport, décembre 2017.
- « Comment permettre à l'homme de garder la main ? Les enjeux éthiques des algorithmes et de l'intelligence artificielle », 2017.

- « La forme des choix. Données personnelles, design et frictions désirables », Cahiers IP Innovation et prospective, 2019, n°06.

- « Les enjeux économiques de la mise en œuvre du règlement sur la gouvernance des données », étude économique destinée aux professionnels, 2023.

Commission nationale de l'informatique et des libertés et Commission d'accès aux documents administratifs en association avec Etalab, « Guide pratique de la publication en ligne et la réutilisation des données publiques ("open data") », publié le 17 octobre 2019.

Commission nationale de l'informatique et des libertés et Commission d'accès aux documents administratifs, « Guide pratique de la publication et de la réutilisation des données publiques », 2016.

Conseil d'État ;

- « Internet et les réseaux numériques », Paris, 1998.

- « Les autorités administratives indépendantes », Rapport public 2001, La Documentation française, 2001.

- « Le droit souple », Rapport annuel, 2013.

- « Le numérique et les droits fondamentaux », étude annuelle, 2014.

- « Mesurer l'inflation normative », étude présentée le 3 mai 2018.

- Rapport « S'engager dans l'intelligence artificielle pour un meilleur service public », Actualités, 30 août 2022.

Conseil d'État et Cour de cassation, De la régulation à la compliance : quel rôle pour le juge ?, Regards croisés du Conseil d'État et de la Cour de cassation, 2024.

Conseil de l'Europe ;

- « La convergence technologique, l'intelligence artificielle et les droits de l'homme », Recommandation 2102 (2017).

- « Lignes directrices sur l'intelligence artificielle et la protection des données », 25 janvier 2019.

- « Recommandation sur les impacts des systèmes algorithmiques sur les droits de l'homme », 2020.

Corporate Europe Observatory, « The lobby network: Big Tech's web of influence in the EU Corporate Europe Observatory », Rapport, 2021.

EDPB et CEPD, Avis conjoint sur la proposition du règlement sur la gouvernance européenne des données (acte sur la gouvernance des données), n° 03/2021, 10 mars 2021.

Gélard Patrice, « Les autorités administratives indépendantes : évaluation d'un objet juridique non identifié », Rapport n° 404 (2005-2006), déposé le 15 juin 2006.

Gélard Patrice, « Autorités administratives indépendantes – 2006-2014, un bilan », Rapport d'information n° 616, déposé le 11 juin 2014.

Groupe de travail de l'article 29 sur la protection des données ;

- Avis n°03/2013 sur le principe de finalité, 00569/13/EN, WP 203, adopté le 2 avril 2013.

- « Avis 05/2014 sur les techniques d'anonymisation », 10 avril 2014.

- « Lignes directrices relatives au droit à la portabilité des données », 16/FR, WP 242.

- « Avis 06/2014 sur la notion d'intérêt légitime poursuivi par le traitement des données au sens de l'article 7 de la directive 95/46/CE », WP 217, 9 avril 2014.

- « Lignes directrices sur l'application et la fixation des amendes administratives aux fins du règlement (UE) 2016/679 », WP253, adoptées le 3 octobre 2017.

- « Lignes directrices sur le consentement au sens du règlement 2016/279 », WP259, 10 avril 2018.

« Avis 06/2014 sur la notion d'intérêt légitime poursuivi par le responsable de traitement au sens de l'article 7 de la directive 95/46/CE », WP 217, 9 avril 2014.

La Haute Autorité pour la diffusion des œuvres et la protection des droits sur Internet et Conseil Supérieur de l'Audiovisuel, Rapport « Assistants vocaux et enceintes connectés, l'impact de la voix sur l'offre et les usages culturels et médias », publié le 28 mai 2019.

Misson Bothorel, « Pour une politique publique de la donnée », 2020.

Mouton Sevane, Benyamina Amine, Bernard Jonathan, G'Sell Florence, Zolynski Célia *et al*., « Enfants et écrans. À la recherche du temps perdu », Rapport remis au Président de la République, avril 2024.

Nicolas Anciaux, Philippe Pucheral, Martine Behar-Touchais, Valérie-Laure Benabou, Geoffray, Brunaux, *et al*., « Contenus numériques », Dossier, 2017.

Pignatelli Chiara et Petitjean Olivier, « GAFAM Nation. La toile d'influence des géants du web en France », Rapport, 2022.

Rouvroy Antoinette et ColinJean-Noël, « Des données et des Hommes. Droits et libertés fondamentaux dans un monde de données massives. », Conseil de l'Europe, 2016.

Sénat, « La protection des données personnelles dans l'open data : une exigence et une opportunité », Rapport d'information.

Sonnac Nathalie, « Rapport d'activité du comité d'éthique sur les données d'éducation », 2020-2021.

Van den Abeele Eric, « "One in, one out" dans le système juridique de l'Union Européenne, une réforme trompe l'œil ? », Working Paper, Institut syndical européen, avril 2020.

Verdier Henri, « La donnée comme infrastructure essentielle », Rapport au premier ministre sur la donnée dans les administrations, 2016-2017.

Villani Cédric, « Donner un sens à l'intelligence artificielle », Rapport, 28 mars 2018, issu de la mission parlementaire sur la mise en œuvre d'une stratégie française et européenne en intelligence artificielle.

Vivant Michel, « Internet et les nouveaux services », Rapport de synthèse du sommet mondial des régulateurs, Paris, 1999.

Waserman Sylvain, « Propositions pour un lobbying plus responsable et transparent », Rapport, présenté par le Vice-président de l'Assemblée nationale Président de la délégation du Bureau chargée des représentants d'intérêts et des groupes d'études, 2021.

VII. Table chronologique des décisions, arrêts, jugements

A) Cour de Justice de l'Union européenne :

Cour de justice des communautés européennes, aff. 6/64, Costa c/ Enel, 25 mars 1957.

Cour de justice des communautés européennes, aff. 106/77, 9 mars 1978.

Cour de justice des communautés européennes, aff. C-101, Bodil Lindqvist, 6 novembre 2003.

Cour de justice des communautés européennes, aff. C-275/06, Promusicae, 29 janvier 2008.

Cour de justice de l'Union européenne, aff. C-161/07, 22 décembre 2008.

Cour de justice de l'Union européenne, aff. C-145/09, 23 novembre 2010.

Cour de justice de l'Union européenne, aff. C-131/12, Google Spain SL et Google Inc. / Agencia Espanola de Proteccion de Datos et Gonzales, 13 mai 2014.

Cour de justice de l'Union européenne, aff.C-507/17, 24 septembre 2019.

Cour de justice de l'Union européenne, aff. C-673/17, Bundesverband c/ Planet 49, 1er octobre 2019.

Cour de justice de l'Union européenne, aff. C-311/18, DPC c/ Facebook Ireland Ltd et M. Schrems, 16 juilet 2020.

Cour de justice de l'Union européenne, aff. C-306/21, Komisia za zashtita na lichnite danni, Tsentralna izbiratelna komisia c/ Koalitsia « Demokratichna Bulgaria – Obedinenie, 20 oct. 2022.

Cour de justice de l'Union européenne, n° C-132/21, Budapesti Elektromos, 12 janvier 2023.

Cour de justice de l'Union européenne, aff. C-300/21, Österreichische Post, 4 mai 2023.

Cour de justice de l'Union européenne, aff. C-634/21, Schufa Holding AG, 7 décembre 2023.

Cour de Justice de l'Union européenne, aff. C-340-21, 14 décembre 2023.

Cour de Justice de l'Union européenne, aff. n° C-465/20, 10 septembre 2024.

B) Décisions du Conseil constitutionnel

Conseil constitutionnel, décision n° 2009-580 DC, 10 juin 2009.

Conseil constitutionnel, décision n° 2020-801 DC du 18 juin 2020.

C) Conseil d'État :

Conseil d'État, aff. Société Faiversta International GMBH, n° 368082, 21 mars 2016.

Conseil d'État, aff. Société NC Numericable, n° 390023, 21 mars 2016.

Conseil d'État, aff. n° 393714, Société JC Decaux, 8 février 2017

Conseil d'État, aff. n° 433069, 16 octobre 2019.

Conseil d'État, aff. n° 401258, 6 décembre 2019.

Conseil d'État, aff. n° 399922, 27 mars 2020.

Conseil d'État, aff. GISTI, n° 418142, 12 juin 2020.

Conseil d'État, n°430810, 19 juin 2020.

Conseil d'État, aff. n° 434684, 19 juin 2020.

Conseil d'État, aff. n° 449209, 28 janvier 2022.

D) Délibérations de la Commission nationale de l'informatique et des libertés

CNIL, délibération n° SAN-2016-054, 10 mars 2016.

CNIL, délibération n° SAN-2017-299, 8 mars 2017.

CNIL, décision n° SAN-2017-075, 27 novembre 2017.

CNIL, délibération n° SAN-2018-349, 15 novembre 2018.

CNIL, délibération n° SAN-2019-001, 21 janvier 2019.

CNIL, délibération n° SAN-2019-160, 21 novembre 2019.

CNIL, délibération n° SAN-2020-091 du 17 septembre 2020.

CNIL, délibération n° SAN-2020-092 du 17 septembre 2020.

CNIL, délibération n° SAN-2020-012, 7 décembre 2020.

CNIL, délibération n° SAN-2020-013, 7 décembre 2020.

CNIL, délibération n° SAN-2020-013, 7 décembre 2020.

CNIL, délibération n° SAN-2021-008, 14 janvier 2021.

CNIL, délibération de la formation restreinte n° SAN-2021-023, 31 décembre 2021.

CNIL, délibération de la formation restreinte n° SAN-2022-017, 3 août 2022.

CNIL, délibération de la formation restreinte n° SAN-2022-018, 8 septembre 2022.

CNIL, délibération de la formation restreinte n°SAN-2022-021, 24 novembre 2022

CNIL, délibération de la formation restreinte n° SAN-2022-023, 19 décembre 2022.

CNIL, délibération de la formation restreinte n° SAN-2022-024, 20 décembre 2022.

CNIL, délibération de la formation restreinte n° SAN-2022-027, 29 décembre 2022.

CNIL, délibération n° SAN-2022-026, 29 décembre 2022.

CNIL, n° SAN-2023-009, 15 juin 2023.

CNIL, délibération SAN-2023-021, 27 décembre 2023.

IX. Sites Internet, articles de blog, articles de presse

AFP, « Scandale de Cambridge Analytica : Facebook accepte de payer 725 millions de dollars à la justice », Libération, 22 décembre 2022.

Benabou Valérie-Laure, « Bannir Trump de Facebook et Twitter, so what ? », Le Club des Juristes, 6 juillet 2021.

Bloch-Wehba Hannah, « Global Platform Governance : Private Power in the Shadow of the State », SMU Law Review, Volume 72, 2019.

Braun Élisa, « Les « dark patterns » : comment les technologies nous manipulent », Le Figaro, publié le 4 juillet 2018.

Bouckaert Colette, « Le règlement DMA : un texte novateur avec des faiblesses », iDFRights, publié le 25 avril 2022.

Bouckaert Colette et Cavada Jean-Marie, « L'Irlande est-elle un frein à l'application du RGPD en Europe ? », IDFRights, publié le 13 juin 2023.

Brewster Jack, Arvanitis Lorenzo et Sadeghi McKenzie, « Le prochain super propagateur d'infox », NewsGuard.

Cadwalladr Carole, « Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach », The Guardian, 17 mars 2018.

Chatelain Yannick, « La censure par invisibilisation des « démocraties » ? Le phénomène du « Shadow Banning », Forbes, 2 avril 2024.

Couderc Lénaïc, « Data, big data, open data », Regards croisés sur l'économie, La Découverte, n° 23, 2018.

De Gregorio Giovanni, « The normative Power of Artificial Intelligence », Indiana Journal of Global Legal Studies, n° 55, 2023.

De Nebehay Marin, « De l'intérêt d'un débat sur la gouvernementalité algorithmique », IDFRights, publié le 27 octobre 2022.

Dechaux Delphine, « Comment Google et les Gafa ont tissé leurs réseaux d'influence à Bruxelles », Challenges, 2019.

Dumoulin Sébastien, « RGPD : la CNIL inflige une amende historique à Google », Les échos, 21 janvier 2019.

Chaudet Bruno, « Donnée, information, connaissance », Logiques processuelles, 30 mars 2009.

Encelot Marjorie, « Les Gafam, ces superpuissances qui peuvent faire dérailler les bourses mondiales », Les échos, 19 juin 2017.

Fagot Vincent, « Face à des missions étendues, la CNIL revendique plus de moyens », Le Monde, 10 avril 2018.

Gaudiat Tristian, Statista, « Lobbying : les Big Tech dépensent des millions en Europe », Statista.

Gavard Emmanuel, « La CNIL change de ton avec les entreprises de la tech », Stratégies, 16 janvier 2023.

Grind Kirsten, Schechner Sam, McMillan Robert et West John, « How Google interferes with its algorithms and changes your results », The Wall Street Journal, 15 novembre 2019.

Hardouin-Ayrinhac Marie-Lou, « Cookies : sanction de 35 millions d'euros à l'encontre d'Amazon Europe Core », Le Quotidien, décembre 2020.

Le Monde, 14 mai 2023.

Le Monde, « De nouveaux documents détaillent le lobbying de Facebook », 4 mars 2019.

Leloup Damien « Facebook accusé de conserver des données effacées », Le Monde, 24 octobre 2011

Leloup Damien, « Cinq ans après le RGPD, des GAFAM ménagés par la CNIL irlandaise »,

Lepilleur Sarah, « Le DSA-DMA fait bondir les dépenses de lobbying des Gafa à Bruxelles », Les Echos, 31 août 2021.

Lesnes Corine, « « L'ex-lobbyiste américaine « Fiona Scott Morton est un cheval de Troie pour Big Tech » à la Commission européenne », Le Monde, 17 juillet 2023.

Letteron Roseline, « La haine sur internet, ou la police exercée par les GAFA », publié sur le blog Liberté, Libertés chéries, 10 juillet 2019.

Petel Antoine, « Politique sur les données : comparaison des approches française et européenne », IDFRights.

Piquard Alexandre, « Facebook : une amende de 5 milliards de dollars et de nouveaux garde-fous, déjà contestés », Le Monde, 24 juillet 2019.

Rivière Pascal, « Qu'est-ce qu'une donnée ? Impact des données externes sur la statistique publique », Courrier des statistiques, n°5, 2020.

Ronfault Lucie « RGPD : la CNIL impose à Google une sanction record de 50 millions d'euros », Le Figaro, 21 janvier 2019

Rosenberg Matthew, Confessore Nicholas et Cadwalladr Carole, « How Trump Consultants Exploited the Facebook Data of Millions », The New York Times, 17 mars 2018.

Schmitt Fabienne, « Meta écope d'une amende record de 1,2 milliard pour transfert illégal de données », Le Figaro, publié le 22 mai 2023.

Schmitt Fabienne et Piquard Alexandre, « Infographie : des GAFA plus puissants que jamais », Le Monde, 19 février 2022.

Schrems Max, « Le RGPD a une influence parce qu'il est et continuera d'être le standard mondiale »», Le Monde, 25 mai 2023.

Sunstein Cass, « Impersonal Default Rules vs. Active Choices vs. Personalized Default Rules : A Triptych », 19 mai 2013.

Untersinger Martin et Clairouin Olivier, « Meta condamné à une amende record de 1,2 milliards d'euros par le régulateur irlandais des données personnelles », Le Monde, 22 mai 2023.

Vinocur Nicholas « We have a huge problem : European tech regulator despairs over lack of enforcement », Politico, 28 décembre 2019.

Index

Les numéros renvoient au numéro de paragraphe

A

Algorithme :
- algocratie : 35
- définition : 9
- discrimination algorithmique 317, 537, 538
- gouvernementalité algorithmique : 536
- prison algorithmique : 70

Altruisme : 130, 311,
Anonymisation :
- notion : 170 et s.
- risques : 181, 184, 622

ARCOM : 400
Asymétrie :
- Informationnelle : 502, 580

Autodérmination
- Informationnelle : 202, 208, 325, 492

Autorégulation : 37, 102, 224, 231
Autorité administrative indépendante : 403, 413
Autorité chef de file : 556 et s., 605

B

Bac à sable réglementaire : 324
Base de données : 200
Big Data : 7, 8, 56, 184, 515, 517 et s., 622
Boîte noire : 539
Bulle de filtre : 69

C

CADA : 162 et s., 399,
Capitalisme de surveillance : 14, 19, 20
Censure : 101, 287, 358
CEPD : 398, 414, 417, 553
Charte des droits fondamentaux : 201, 438, 477
Chef de file : v. autorité chef de file
CNIL :
- Autorité de contrôle : 398, 550, 597

- Autorité de supervision : 552
- Bilans : 593
- Moyens : 612
- Pouvoirs : 404, 407, 463, 551,
- Recours : 559

Code de conduite : 376, 378
Compliance : 421 et s.
Consentement :
- « consentement vulnérable » : 494 et s.
- « consentement superficiel » : 504 et s.
- notion : 455, 476 et s.

Contenus :
- haineux : 94, 95, 96
- illicites : 98 et s.
- numérique : 16, 73 et s.
- privatisation (de la modération) : v. privatisation
- terroristes : 92, 93

Cookies : 67, 113, 252, 263, 279, 428, 491, 504 et s.
Coopération : 414 et s.
Corégulation : 376
Courtiers de données : 65, 310, 541

D

Data Act : 230, 294, 303 et s.
Data broker : v. courtiers de données
Data Governance Act : 51, 130, 162, 300 et s., 407, 442,
Data Privacy Framework : 22
Décisions automatisées : 461, 532 et s.
Deep learning : 61, 357, 521
Digital Market Act : 262, 268 et s. 292, 444
Digital Service Act : 98, 262, 281 et s., 444
Dommage :
- moral : 575 et s.
- notion : 568, 573 et s.

Données :
- composites : 157
- définition générale : 48
- définition légistique : 51
- étymologie : 47
- mixtes : 154 et s.
- naturelles : 4
- numériques : 5
- pseudonymisée : v. pseudonymisation

- sémantiques : 87
- usage : 56, 59, 63, 64, 74, 202
- volume : 6, 134, 181

Données à caractère non personnel : 114 et s.
Données à caractère personnel :
- anonymisée : v. anonymisation
- doctrine patrimoniale : 197 et s.
- doctrine personnaliste : 200 et s.
- droit fondamental : 27, 434, 438

Données altruistes : 130
Données biométriques : 119
Données commerciales : 280
Données d'éducation : 127
Données d'intelligence artificielle : 131
Données de « bien être » : 124, 125 et 126
Données de santé : 120
Données génétiques : 119
Données industrielles : 28, 115, 303
Données preuve : 129
Données publiques :
- d'intérêt général : 144
- de référence : 141
- définition : 138
- forte valeur :147
- open data : v. open data
- service public : v. service public de la donnée

Données sensibles : 118 et s.
Droit à l'oubli : 204 et s.
Droit à la portabilité : 208 et s.
Droit au déréférencement : v. droit à l'oubli
Droit de portage : 223
Droit de propriété :
- sur information : v. information
- sur les données : v. donnée

Droit global : 363

E

Économie de l'attention : 15 et s., 69, 82
Empowerment : 208, 478
Environnement :
- impact : 24, 236,
- instabilité : 31
- technique : 324, 362

Éthique : 312, 314

F

Facebook : 13, 16, 17, 23, 67, 100, 257, 277, 286, 358, 454, 492, 499, 530, 542, 598, 609, 610
Faute : 567 et s.
Filter bubble : v. bulle de filtre
Flux de données : 26, 31, 55, 115, 220
Flux normatif : 237

G

GAFAM : 12, 29, 36, 64, 197, 254 et s.,
Gatekeeper : 276, 355
Google
- droit au déréférencement : 204
- lobbying : 256 et s.
- publicité : 67, 83, 286
- sanctions : 432, 509, 595,

Gouvernance : 299 et s., 325, 365 et s.,
Gouvernementalité :
- algorithmique : v. algorithme

Groupe de pression : v. lobbying
Guichet unique : v. autorité chef de file

I

Idéalisme : 25, 619
Identité : 110, 200
Information : 47, 49, 58, 87, 111 et s., 202, 214, 500
Intelligence artificielle :
- définition : 9, 61, 131
- générative : 103

Intelligence Artificiel Act : 131, 313, 327

Interface trompeuse : 288, 506
Interrégulation : 409 et s.

J et L

Juge administratif : 557
Liberté d'expression : 95, 101, 358
Liberté de circulation :
- des données à caractère non personnel : 219 et s.
- des données à caractère personnel : 28, 110,

Lobbying : 36, 245 et s.

M et N

Machine learning : 61, 520
Manipulation : 70, 102, 278, 504 et s.
Marché unique des données : 189
Marché unique numérique : 29, 188 et s. 219
Marketing : 64, 519
Modération : 102, 287, 358
Monopole : 2, 67, 267, 271, 273
Mineur : 17, 289, 455
Minimisation : v. principe de minimisation
Netflix : 87, 183
NIR : 123

O

Objets connectés : 8, 14, 28, 55, 124, 294, 303, 517
Omniconnexion : 5 et s.
Opacité : 33, 290, 236, 461, 533 et s., 540,
***Open data* :** 136 et s., 163, 214 et s., 301, 441

P

Pluralisme normatif : 240
Principe de finalité : 323, 449, 470, 523 et s.
Principe de minimisation : 322, 470, 523 et s.
Principe de transparence : 282 et s., 325, 534
PRISM : 21
Privacy shield : 22
Privatisation :
- de la modération : 100 et s.
- des données de bien être : 126
- des normes : 352 et s., 389
- du reseau : 2

Profilage : 327, 444, 504, 533
Pseudonymisation : 169
Publicitée ciblée : 67, 82, 289, 444
Pyramide des normes : 361 et s., 381

R

Recours : 428, 559 et s.
Réseau de normes : 373
Responsabilité : 509, 530, 566 et s.

S

SAFARI : 27, 193
Safe Harbor : 22
Schrems : 22, 530
Service d'intermédiation de données : 310, 448
Service public de la donnée : 142
Signaleur de confiance : 287
Sous-traitant : 540, 561, 568, 571
Souveraineté : 26, 241
Surveillance :
- Snowden : 21
- Société (de) : 14, 19, 20, 328, 346

T et V

Transfert de données : 22, 543
Transparence : 33, 248, 281, 288, 325
Valeur d'usage : 59, 64, 137
Vie privée : 8, 27, 163, 166, 201, 235, 445

Table des matières

Remerciements

Liste des abréviations

Sommaire

INTRODUCTION GÉNÉRALE 2

PARTIE 1 : 40

L'ÉLABORATION D'UN CADRE NORMATIF COMPLEXE 40

TITRE 1 : LA DIVERSITÉ ÉVOLUTIVE DES NOTIONS 42

Chapitre 1 : La notion de données et les notions voisines : divergences et convergences 44

Section 1 : La notion de donnée et la notion d'information 44

I. La polysémie des notions 44

A) La confusion des notions 44

1. L'étymologie des notions 45

47. Étymologie équivoque des notions 45

2. Définition légistique des données 47

B) La distinction des notions 48

1. La nature ambivalente des données 48

2. Les sources des données 50

II. La construction de l'information 51

A) L'analyse et l'exploitation des données 51

1. L'analyse des données 51

2. L'exploitation des données 55

B) Les risques de l'exploitation des données 58

1. Le modèle économique des plateformes 58

2. Les risques pour les utilisateurs 60

Section 2 : Les notions de données et de contenus 64

I. La notion positive de contenu : des données interprétées 64

A) La valeur des contenus 64

1. La polysémie de la notion de contenu 65

2. L'intérêt économique des contenus 67

B) Le déplacement de valeur 70

1. La contribution de la valeur par les internautes 70

2. La captation de la valeur par les plateformes 71

II. La notion négative de contenu : les contenus illicites 73

A) Les notions de contenus haineux et à caractère terroriste 73

1. Les contenus à caractère terroriste 73

2. Les contenus haineux 75

B) Les contenus illicites 77

1. La notion large de contenu illicite 77

2. La privatisation de la notion du contenu illicite 78

Chapitre 2 : 84

La notion juridique de données : forces et faiblesses 84

Section 1 : L'instauration d'une typologie des données 84

I. Les notions de données à caractère personnel et données à caractère non personnel 84

A) Les définitions des données à caractère personnel et non personnel 84

1. Définition large de la donnée à caractère personnel 85

2. Définition par opposition de la donnée à caractère non personnel 88

B) Les catégories particulières de données 90

1. Les données sensibles 90

2. Les notions de données novatrices 94

II. La construction de la notion des « données publiques » 100

A) La définition stricte de la donnée publique 100

1. Contexte de la donnée publique 101

2. Notion de donnée publique 103

B) Les définitions concurrentes à la notion de donnée publique 104

1. La notion de « données de référence » 104

2. La notion de « données d'intérêt général » 106

Section 2 : L'instabilité de la typologie 111

I. Le chevauchement des notions 111

A) Les données à caractère personnel et données à caractère non personnel 112

1. La notion d'« ensemble de données mixtes » 112

2. L'application de règles distributives 114

B) Les données à caractère personnel et les données publiques 116

1. L'encadrement des données ouvertes 116

2. La recherche d'un équilibre entre ouverture et protection 118

II. Les faiblesses de l'anonymisation 120

A) Le principe de l'anonymisation 120

1. Notions d'anonymisation et de pseudonymisation 121

2. Les techniques d'anonymisation 124

B) Les limites du principe d'anonymisation 127

1. Le contexte de Big Data 127

2. Les limites des techniques 128

TITRE 2 : L'EXCESSIVE DIVERSITÉ DES NORMES 134

Chapitre 1 : L'établissement d'un cadre ambivalent pour les données 137

Section 1 : La recherche utopique d'un équilibre entre ouverture et protection des données 138

I. La protection des données à caractère personnel face à l'exploitation abusive 139

A) La protection de la personne contre l'exploitation abusive 139

1. L'inopportunité de l'analyse patrimoniale 139

2. L'opportune consécration de l'analyse personnaliste 142

B) Les faiblesses de certains droits face à l'exploitation abusive 145

1. Les restrictions territoriales du droit à l'effacement 146

2. Les limites techniques du droit à la portabilité 149

II. L'ouverture des données à caractère non personnel face à la concentration abusive 151

A) Les prémisses de la politique d'ouverture des données à caractère non personnel 151

1. Le développement de la politique d'open data pour les données publiques 152

2. L'instauration du principe de libre circulation pour les données à caractère non personnel 156

B) L'essoufflement prématuré de la politique d'ouverture des données à caractère non personnel 160

1. Les difficultés pratiques d'ouverture des données à caractère non personnel 160

2. Le bilan insatisfaisant du principe d'ouverture des données à caractère non personnel 163
Section 2 : Les conséquences de la recherche d'un équilibre utopique 166
I. La multiplication excessive des normes 166
A) La profusion des normes 166
1. La transversalité du droit des données 166
2. Les flux normatifs pour les données 169
B) La dispersion des normes 171
1. Le pluralisme normatif 171
2. L'altération de la cohérence des normes 172
II. La multiplication des influences scabreuses 174
A) L'influence collective des groupes de pression 174
1. La relation d'interdépendance entre le législateur et les groupes de pression 174
2. Les effets pervers de la relation d'interdépendance 178
B) L'influence spécifique des acteurs du numérique 180
1. L'influence néfaste des GAFAM 180
2. L'influence incontestable des GAFAM 183

Chapitre 2 : L'émergence d'un cadre concurrentiel pour les données 191
Section 1 : Le recours à une réglementation ciblée contre l'accumulation massive des données 191
I. Une réglementation contre l'accès asymétrique aux données 191
A) L'adaptation de l'approche traditionnelle du droit de la concurrence 192
1. L'inadéquation du droit de la concurrence au marché des données 192
2. L'émergence d'une réglementation concurrentielle de la donnée 195
B) La nouvelle approche ciblée contre l'accès asymétrique des données 196
1. La qualification asymétrique des contrôleurs d'accès 197
2. L'interdiction de combinaison et de croisement des données à caractère personnel des utilisateurs 198
II. Une réglementation renforcée favorable aux utilisateurs 200
A) Le renforcement insuffisant de l'obligation de transparence pour les plateformes dominantes 200
1. L'adaptation nécessaire des catégories de plateformes aux géants du numérique 201
2. L'adaptation insuffisante des mesures aux risques en ligne 203
B) L'importance du renforcement de la portabilité des données pour les utilisateurs 206
1. La consécration d'une portabilité effective des données fournies ou générées 207
2. La création d'une portabilité renforcée des données générées par les objets connectés 208
Section 2 : L'objectif chimérique d'une réglementation globale pour l'ouverture des données 211
I. L'élaboration d'un modèle disruptif de partage des données 211
A) La mise en place d'une gouvernance de confiance 212
1. Le renouvellement de la politique d'ouverture des données publiques 212
2. La récente mise à disposition des données industrielles 214
B) La mise en place d'un écosystème de confiance 216
1. Le développement d'un partage de confiance 216
2. Le développement d'une intelligence artificielle de confiance 219
II. Les conséquences de l'ouverture excessive des données 224
A) L'altération progressive de la protection des données à caractère personnel 225
1. La primauté du potentiel économique sur les enjeux de protection 225
2. L'adaptation à risque des principes protecteurs au nom de l'innovation 227
B) La protection chimérique des utilisateurs contre les SIA à haut risque 228
1. L'utopique principe de transparence 229
2. L'utopique protection des individus 231

PARTIE 2 : 243

LA MISE EN ŒUVRE LACUNAIRE DU CADRE NORMATIF 243

TITRE 1 : L'ARTICULATION ARTIFICIELLE DES NORMES 245

Chapitre 1 : Le modèle pyramidal pour le droit des données : une vision archaïque 247

Section 1 : Les limites de la logique hiérarchique pour le droit des données 248

I. L'indispensable européanisation du droit des données 248

A) L'hégémonie nécessaire du droit européen pour l'élaboration des normes 248

1. Le principe de primauté du droit communautaire 248

2. L'européanisation du droit des données 250

B) La marginalisation inévitable de l'État pour l'élaboration des normes 251

1. L'inflexion de la place de l'État 251

2. La progression de la législation déléguée 253

II. La privatisation subreptice du droit des données 253

A) La construction participative des normes 254

1. La participation des organismes privés 254

2. L'intégration de la norme dans le code informatique 255

B) La constitution d'un réseau complexe de normes 259

1. L'obsolescence de la pyramide des normes 259

2. La substitution de source par le pouvoir 260

Section 2 : La nouvelle logique de gouvernance du droit des données 263

I. La prépondérance du droit souple pour la gouvernance 264

A) L'inflation vertigineuse du droit souple 264

1. La prééminence des autorités administratives indépendantes pour la régulation des données 264

2. La prolifération des actes de régulation des données 266

B) L'influence décisive du droit souple 268

1. L'intégration du droit souple dans la loi 268

2. La création d'un droit souple « contraignant » 269

II. Les risques de la prééminence du droit souple 270

A) L'incertaine frontière entre droit souple et droit dur 270

1. La reconnaissance de force normative des actes de droit souple 271

2. La dilution de la norme dans l'ordre juridique 272

B) Les dangers de la co-production du droit 273

1. L'intégration d'intérêts mercantiles dans l'élaboration des normes 273

2. L'intégration des acteurs dans le système de normes 275

Chapitre 2 : Le modèle du réseau de normes pour les données : un outil de subversion 280

Section 1 : L'articulation flexible des mécanismes de régulation 280

A) La multiplicité dynamique des autorités administratives indépendantes 281

1. La diversité excessive des autorités administratives indépendantes 281

2. La diversité évolutive des pouvoirs des autorités de régulation 284

B) La constitution progressive d'un système de régulation en réseau 289

1. L'inévitable mécanisme d'interrégulation au niveau national 289

2. L'innovant mécanisme de coopération au niveau européen 293

II. L'articulation subtile des divers instruments normatifs 297

A) La mise en place innovante d'un système de compliance 297

1. L'internalisation utopique des normes par les acteurs 298

2. La perspective indispensable d'une sanction pour les acteurs 301

B) L'indispensable contrôle du juge pour la cohérence du système 303

1. Le contrôle des actes des autorités administratives indépendantes 303
2. Le contrôle juridictionnel des sanctions des autorités administratives indépendantes 306
Section 2 : L'articulation superficielle des mécanismes de protection des données à caractère personnel 310
I. La superficielle prévalence de la protection des données à caractère personnel à travers les réglementations 311
A) La prévalence incontestable du RGPD dans la hiérarchie des normes des données 311
1. La prévalence fondamentale de la protection des données à caractère personnel 311
2. La prévalence textuelle du règlement (UE) 2016/679 313
B) La prévalence contestable du RGPD en pratique 317
1. Le chevauchement des régimes 318
2. Le bouleversement des usages 320
II. L'extension artificielle de la protection des données à caractère personnel 321
A) La normativité protectrice du législateur 322
1. L'usage des marges de manœuvre par le législateur 322
2. Les difficultés d'articulation 324
B) L'interprétation extensive du cadre normatif 326
1. L'appréciation extensive de la protection des individus par la Cour de justice de l'Union européenne 326
2. L'extension des pouvoirs normatifs des autorités par la SREN 330

TITRE 2 : L'EFFECTIVITÉ LIMITÉE DU CADRE NORMATIF 337

Chapitre 1 : 339

Les limites de l'effectivité des règles 339
Section 1 : Le principe limité du consentement face aux pratiques des géants du numérique 340
I. Le renforcement du principe en théorie 340
A) La notion spécifique du consentement 340
1. La définition précise du consentement 341
2. Les caractères du consentement valable 343
B) La valeur surestimée du consentement 347
1. Une notion concurrencée 348
2. Une notion surestimée 350
II. L'application illusoire du consentement en pratique 352
A) Un « consentement vulnérable » pour les utilisateurs 352
1. La gratification immédiate 353
2. L'asymétrie informationnelle 356
B) Un « consentement superficiel » pour les acteurs du numérique 358
1. La manipulation du consentement 358
2. L'alternative de l'intérêt légitime 363
Section 2 : Les principes de protection face à la réalité technologique 366
I. L'inadéquation des principes de protection à l'ère du Big Data 366
A) L'expansion du phénomène 367
1. L'essor des opportunités du Big Data 367
2. Les outils d'analyse de données 368
B) Le recul de la protection 370
1. Les limites des principes de finalité et de minimisation 370
2. Les limites du droit à l'effacement 373
II. Les risques de l'inadéquation des principes de protection 375
A) Les effets néfastes des décisions automatisées pour les individus 375
1. L'opacité des algorithmes d'apprentissage automatique 375

2. Les risques de l'utilisation des algorithmes 378
B) La transmission obscure des données à caractère personnel à des tiers 380
1. L'opacité des pratiques des sociétés d'analyse des données 381
2. L'inconscience des utilisateurs de l'existence des sociétés 382

Chapitre 2 : 388

Les limites de l'effectivité des sanctions 388
Section 1 : La complexité du régime répressif pour les personnes concernées 389
I. La complexe mise en œuvre du régime répressif 389
A) La multiplicité excessive des acteurs 389
1. Les acteurs spécialisés 389
2. Les acteurs de droit commun 394
B) La diversité évolutive des recours 395
1. Les recours auprès d'une autorité de contrôle 395
2. Les recours contre un responsable de traitement ou un sous-traitant 397
II. La construction incertaine du régime répressif 400
A) Le fait générateur de responsabilité : une notion simplifiée 400
1. La nature de la responsabilité 400
2. Le partage de la responsabilité 403
B) La réparation du dommage : une notion en construction 404
1. La difficulté d'évaluation du dommage 404
2. Les difficultés probatoires du préjudice 409
Section 2 : L'inégale mise en œuvre du régime répressif par les différentes autorités de contrôle 412
I. L'intensification variable de l'activité répressive des autorités de contrôle 413
A) L'appréciation variable des sanctions 413
1. Une appréciation variable 413
2. Une appréciation cohérente 415
B) Les disparités d'application des sanctions 417
1. L'action affirmée de la Commission nationale de l'informatique et des libertés 417
2. L'action inégale des homologues de la CNIL 422
II. L'impuissance des autorités de contrôle face à la puissance des multinationales 426
A) La puissance des multinationales face aux autorités de contrôle 426
1. Une domination publique 426
2. Des intérêts privés 429
B) L'impuissance des autorités de contrôle face aux géants du numérique 430
1. Le manque de moyens des autorités de contrôle 431
2. L'insuffisance des sanctions 432

CONCLUSION GÉNÉRALE 441

Bibliographie 445

Index 495

Table des matières 501

Université de Strasbourg

Déborah HERTZ

Ecole doctorale des sciences juridiques | ED 101
Université de Strasbourg

Le cadre normatif des données : une construction idéaliste ?

Résumé

L'objet de cette étude est d'entreprendre une analyse critique de la construction du cadre normatif des données. Il s'agit de comprendre comment le législateur a appréhendé ce nouvel objet de droit : les données transcendent l'ensemble des matières juridiques et soulèvent de nouveaux enjeux. L'approche transversale de cette étude permet d'identifier le cadre normatif afin d'instaurer une typologie des notions de données et les différents régimes juridiques. L'analyse de l'élaboration du cadre complexe permet d'anticiper sa mise en œuvre et notamment, les difficultés d'articulation et d'effectivité des normes. Plus précisément, l'étude permet d'observer et de démontrer l'influence des acteurs du numérique dans l'élaboration des normes.

Données à caractère personnel – Données à caractère non personnel – Marché unique des données – Lobbying

Résumé en anglais

The purpose of this study is to undertake a critical analysis of the construction of the normative framework for data. It aims to understand how lawmakers have approached this new legal object: data transcends all legal fields and raises new challenges. The cross-sectional approach of this study allows for the identification of the normative framework to establish a typology of data concepts and to associate their legal regime. The identification phase helps anticipate the implementation of the framework, particularly the challenges related to the coherence and effectiveness of the regulations. More specifically, the study aims to observe and demonstrate the influence of digital actors in the development of the normative framework.

Personal data – Non-personal data – Single data market – Lobbying