THÈSE PRÉSENTÉE

POUR OBTENIR LE GRADE DE

DOCTEUR DE

L'UNIVERSITÉ DE BORDEAUX

ÉCOLE DOCTORALE DE DROIT (ED 41)

SPÉCIALITÉ DROIT PRIVE ET SCIENCES CRIMINELLES

Par Malika ONGARO

Le traitement des données à caractère personnel dans le cadre des procédures judiciaires

Sous la direction de Madame le Professeur Aurélie Bergeaud-Wetterwald

Soutenue le 29 mars 2021

Membres du jury :

Madame Aurélie BERGEAUD-WETTERWALD,
Professeur à l'Université de Bordeaux, *directrice de thèse*
Madame Anaïs DANET,
Professeur à l'Université de Reims Champagne-Ardenne, *rapporteur*
Monsieur Xavier DAVERAT,
Professeur à l'Université de Bordeaux, *examinateur*
Monsieur Romain OLLARD,
Professeur à l'Université de Poitiers, *rapporteur*

Titre : Le traitement des données à caractère personnel dans le cadre des procédures judiciaires

Résumé : Au cours des procédures judiciaires, grand nombre de données à caractère personnel sont amenées à intervenir à différents stades et pour divers motifs. Le traitement de données à caractère personnel se trouve encadré par des textes supra nationaux et internes et notamment le règlement général sur la protection des données et la loi informatique et libertés. Ces textes ont réaffirmés et accentués des principes protecteurs pour les individus visés par un traitement de données. S'agissant des procédures judiciaires se posent des interrogations liées à l'exploitation de ces données de part leur valeur probatoire ou informative, nécessitant le fichage de certaines d'entre elles. Le développement du numérique conduit à repenser l'usage des données d'identification. Si les nouvelles technologies constituent des outils utiles à l'administration de la justice, il convient néanmoins de s'interroger sur la protection accordée aux données dans ce nouveau contexte. Au cours des procédures judiciaires, les données à caractère personnel contenues dans les dossiers se trouvent tantôt protégées par un secret, tantôt diffusées par l'application de différents principes processuels ou par les nécessités de la procédure. Une fois la procédure achevée, se pose la question du sort de ces données que ce soit par la gestion des données fichées ou la diffusion des décisions de justice, à l'heure notamment de l'open data. Ces questions renvoient nécessairement à celle du droit à l'oubli qui prend une dimension particulière avec le développement d'internet. Entre nécessité d'informer et protection des données, il convient de s'interroger sur le traitement des données à caractère personnel au cours des procédures judiciaires au regard notamment du droit des données à caractère personnel.

Mots clés : Données personnelles, Fichiers, Preuve, Open data, Droit à l'oubli

---

Title : The processing of personal data in legal proceedings

Abstract : In the course of legal proceedings, a large amount of personal data is collected at different stages and for different reasons. The processing of personal data is regulated by supra-national and national laws, in particular the General Data Protection Regulation and the data protection act. These texts have reaffirmed and accentuated protective principles for individuals concerned by data processing. With regard to legal proceedings, questions arise in relation to the use of this data for its probative or informative value, necessitating the recording of a number of them. The development of digital technology makes it necessary to rethink the use of identification data. If new technologies are useful tools for the administration of justice, it is necessary to consider the protection accorded to data in this new situation. In the course of legal proceedings, the personal data contained in the files are sometimes protected by a secret, sometimes divulged by the application of different procedural rules or by the needs of the proceedings. Once the procedure is closed, the question arises as to the fate of this data, by the management of file data or the diffusion of court judgments, especially in the age of open data. These questions necessarily refer to that of the right to be forgotten, which takes on a new dimension with the Internet. Between the need for information and data protection, questions must be asked about the processing of personal data during legal proceedings, particularly with regard to personal data law.

Keywords : Personal data, Files, Evidence, Open data, Right to be forgotten

Unité de recherche

[Institut de sciences criminelles et de la justice, EA 4633, 4 rue du Maréchal Joffre, 33000 Bordeaux]

« L’Université n’entend donner aucune approbation ni improbation aux opinions émises dans les thèses : ces opinions doivent être considérées comme propres à leurs auteurs. »

Liste des principales abréviations et sigles

Al.	Alinéa
Art.	Article
Ass. plén.	Assemblée plénière
CA	Cour d'appel
CE	Conseil d'Etat
Cons.	Considérant
Cass.	Cour de cassation
Civ.	Chambre civile de la Cour de cassation
CNIL	Commission nationale de l'informatique et des libertés
Cour E.D.H.	Cour européenne des droits de l'homme
Cour J.U.E	Cour de justice de l'Union européenne
Crim.	Chambre criminelle de la Cour de cassation
FAED	Fichier automatisé des empreintes digitales
FNAEG	Fichier national automatisé des empreintes génétiques
G29	Groupe de travail article 29
LIL	Loi informatique et libertés
PNIJ	Plateforme nationale des interceptions judiciaires
QPC	Question prioritaire de constitutionnalité
s.	Suivants
TAJ	Traitement des antécédents judiciaires
TJ	Tribunal judiciaire
RGPD	Règlement général sur la protection des données
RSC	Revue de sciences criminelles
TGI	Tribunal de grande instance
TJ	Tribunal judiciaire

SOMMAIRE

(Plan détaillé en fin de thèse)

INTRODUCTION

PREMIERE PARTIE
L'EXPLOITATION DES DONNEES A CARACTERE PERSONNEL DANS LES PROCEDURES JUDICIAIRES

TITRE 1 : LES DONNEES A CARACTERE PERSONNEL INTERVENANT DANS LES PROCEDURES JUDICIAIRES A TITRE PROBATOIRE

Chapitre 1 : La collecte des données à caractère personnel au regard des principes encadrant la licéité de la preuve

Chapitre 2 : L'impact de la nature particulière des données à caractère personnel sur leur fonction probatoire

TITRE 2 : LES DONNEES A CARACTERE PERSONNEL ALIMENTANT DES FICHIERS JUDICIAIRES

Chapitre1 : La création des fichiers judiciaires

Chapitre 2 : Le partage de données fichées

DEUXIEME PARTIE
LA PROTECTION DES DONNEES A CARACTERE PERSONNEL DANS LES PROCEDURES JUDICIAIRES

TITRE 1 : LES PRINCIPES ENCADRANT LA DIFFUSION DES DONNEES A CARACTERE PERSONNEL AU COURS DE LA PROCEDURE JUDICIAIRE

Chapitre 1 : Les principes limitant la diffusion de données

Chapitre 2 : Les principes justifiant la diffusion de données

TITRE 2 LE SORT DES DONNEES A CARACTERE PERSONNEL COLLECTEES DANS LE CADRE DE PROCEDURES JUDICIAIRES

Chapitre 1 : La gestion de données à caractère personnel collectées dans le cadre d'une procédure judiciaire

Chapitre 2 : Le droit à l'oubli des données à caractère personnel collectées dans le cadre d'une procédure judiciaire

INTRODUCTION

1. Le traitement des données à caractère personnel : une préoccupation grandissante – L'usage fait des données à caractère personnel a toujours suscité des craintes et des interrogations. Foncièrement lié à la notion de vie privée, le traitement de données personnelles reste, dans les esprits, attaché à certains épisodes historiques tels que « l'affaire des fiches »[1] ou le projet Safari[2]. Le fichage des individus de plus en plus massif, au-delà des avancées qu'il permet, soulève des interrogations légitimes sur les excès qu'il pourrait entrainer, laissant craindre pour certains la concrétisation des prédictions de George Orwell en 1949[3] et l'avènement d'une société ultra sécuritaire. Ces craintes sont évidemment liées au développement d'internet et du *big data*[4]. La diffusion massive des données sur internet, leur utilisation et diffusion par les GAFA[5] et le développement de sociétés telles que *Wikileaks*[6] laissent craindre une diffusion de données qui se ferait au détriment des droits des individus concernés.

Le sujet amène à s'interroger sur deux types de traitements des données. D'un côté, la collecte et le fichage par les autorités qui doit trouver le juste équilibre entre le traitement nécessaire à la bonne administration de la justice et les droits des individus. D'un autre côté, le traitement par les organes de presse et les sociétés privées qui de plus en plus diffusent des données personnelles parfois liées à des procédures judiciaires. Il faut dans ce cas trouver l'équilibre entre la liberté d'expression, le droit à l'information et les droits des individus concernés. Face au traitement de données personnelles dans une société de communication qui aspire à la

[1] En référence au scandale qui éclata en 1904, lié au fichage des opinions politiques et religieuses des officiers mis en œuvre par le Général André, ministre de la guerre.

[2] Le projet SAFARI visait la création en 1973 du ficher intitulé « Système Automatisé pour les Fichiers Administratifs et le Répertoire des Individus » qui devait interconnecter les fichiers de l'Administration entrainant de fait le fichage de la population. Face aux vives critiques et oppositions, le projet a été abandonné et a donné lieu à la création de l'organe de contrôle qu'est la CNIL.

[3] G. Orwell, *1984*, Gallimard, 1950 (version traduite). Dans l'ouvrage, l'auteur dépeint le futur trente cinq ans plus tard dans une société totalitaire qui opère une surveillance permanente des individus et fonctionne avec des autorités de contrôle telles que la police de la pensée.

[4] Le terme de Big data peut être traduit par celui de « Mégadonnées » et renvoie au traitement massif de données numériques rendu possible par les nouveaux moyens de communication.

[5] Le terme de GAFA a été créé en référence aux quatre entreprises considérées comme étant les plus puissantes d'internet : Google, Apple, Facebook, Amazon. Si d'autres entreprises sont depuis venues étendre le nombre de ces entreprises, ont conserve le terme de GAFA pour les désigner (parfois GAFAM le « M » désignant Microsoft). Ces entreprises gèrent une quantité massive de données personnelles et sont souvent au cœur de controverses quant à l'utilisation de ces données.

[6] Wikileaks est une organisation non gouvernementale à but non lucratif qui diffuse des données issues de sources anonymes. Fondant son action sur la liberté d'expression, elle se trouve au cœur de litiges liés au fait que les données diffusées peuvent être des données protégées ou des données sensibles.

transparence et au droit à l'information, faut-il craindre *big brother*[7] ou *l'œil de Sauron*[8] ? L'intérêt du sujet est ici d'observer les évolutions qui ont eu un impact sur le traitement des données à caractère personnel en matière judiciaire, d'en mesurer les enjeux et de s'interroger sur cet équilibre parfois délicat entre le traitement nécessaire et la protection des droits des individus.

2. Les données à caractère personnel : une notion vaste – L'idée d'assurer une protection des données personnelles faisant l'objet d'un traitement n'est pas récente. La loi informatique et libertés du 6 janvier 1978 dans sa rédaction initiale visait les « informations nominatives » permettant une identification directe ou indirecte des individus[9].

La Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, signée le 28 janvier 1981 et ratifiée par la France le 24 mars 1983 dite « Convention 108 » vise les données à caractère personnel, les définissant comme toute information relative à des personnes physiques identifiées ou identifiables.

La directive européenne du 24 octobre 1995 va définir les données à caractère personnel comme « toute information concernant une personne physique identifiée ou identifiable »[10] ajoutant « qu'est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale »[11]. C'est cette définition qui va être reprise par la suite à l'article 4 du règlement général sur la protection des données du 27 avril 2016.

Modifiée par la loi du 6 août 2004 qui transpose la directive du 24 octobre 1995, la loi informatique et libertés fait alors référence aux données à caractère personnel permettant l'identification directe ou indirecte par un numéro d'identification ou par « un ou plusieurs éléments propre [à la personne] ». Aussi, le caractère identifiable de l'individu est à observer au regard des moyens à la disposition du responsable du traitement ou de toute personne. Toutefois dans la réécriture de la loi par l'ordonnance du 12 décembre 2018, le législateur a

[7] En référence au roman de George Orwel, *op. cit.*

[8] En référence aux romans de J.R.R. Tolkien, Le seigneur des anneaux, parus en 1954 et 1955, dans lesquels Sauron est une entité capable d'opérer une surveillance permanente et généralisée des individus.

[9] Loi n°78-1 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Art. 4 dans sa rédaction initiale.

[10] Directive n° 95/46/CE du 24 octobre 1995 du Parlement européen et du Conseil 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, art. 2.

[11] *Ibid.*

fait le choix de ne pas reprendre la définition des données à caractère personnel, préférant opérer un renvoi aux dispositions du règlement général sur la protection des données qu'il transpose.

Ainsi, constitue une donnée à caractère personnel, « toute information se rapportant à une personne physique identifiée ou identifiable ; 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 »[12].

La notion de données à caractère personnel renvoie donc à une multitude d'informations. Elle a évolué et s'est précisée pour s'adapter aux évolutions technologiques et notamment aux nouveaux moyens de communication. La donnée personnelle peut être numérique, c'est précisément cette dématérialisation qui a poussé à repenser la protection des données. L'avènement du *big data* permet un échange illimité des données sans contraintes géographiques ni contraintes techniques, celui-ci permettant une communication massive de données.

3. Les données à caractère personnel sensibles : la nécessaire catégorisation des données

– Parmi les données à caractère personnel pouvant faire l'objet d'un traitement il faut distinguer les données dites « sensibles » qui de par leur nature sont soumises à un régime particulier. La directive du 24 octobre 1995 visait les « catégories particulières » de données qui ne pouvaient, sauf exceptions, faire l'objet d'un traitement[13]. La loi informatique et libertés dans une rédaction antérieure visait également la catégorie de données rassemblant les opinions politiques ou religieuses[14].

Ce critère de sensibilité apparait plus clairement dans le règlement général sur la protection des données qui développe l'idée selon laquelle les données sensibles, du fait des risques en termes de droits et libertés pour les individus, doivent nécessairement faire l'objet d'une protection particulière et donc relever de dispositions spécifiques[15]. Dans sa version actuelle, la loi informatique et libertés pose, à l'article 6, le principe de l'interdiction de traitement des

[12] Art. 4 du règlement général sur la protection des données.
[13] Art. 8 de la directive du 24 octobre 1995.
[14] Art. 8 de la loi informatique et libertés dans sa version antérieure à l'ordonnance du 12 décembre 2018 et faisant suite à l'adoption de la loi du 6 août 2004 (n°2004-801).
[15] Cons. 51 du règlement général sur la protection des données.

données « qui révèlent la prétendue origine raciale ou l'origine ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale d'une personne physique »[16]. Il est également interdit de traiter « des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique »[17]. Cette interdiction connait néanmoins des exceptions prévues par la loi et le règlement, le traitement de données sensibles pouvant s'avérer nécessaire.

Ce critère de sensibilité des données tel que définit par les textes est important en ce qu'il influe sur les normes applicables en termes de traitement. Ces données relèvent d'un régime particulier qui appelle une protection renforcée et soumet le traitement à des conditions plus strictes. Ces particulièrement cette catégorie de données qui soulève dans la pratique de vives interrogations.

4. Le traitement de données à caractère personnel : une notion diffuse – Les textes relatifs à la protection des données à caractère personnel ont vocation à s'appliquer aux traitements automatisés ou non automatisés de données contenues dans des fichiers ou ayant vocation à alimenter des fichiers. La notion de traitement a finalement peu évolué.

La loi informatique et libertés dans sa version initiale faisait référence à « tout ensemble d'opérations »[18], notion reprise dans la directive du 24 octobre 1995 qui vise « toute opérations ou ensemble d'opérations »[19]. La loi informatique et libertés renvoie désormais à l'article 4 du règlement général sur la protection des données s'agissant de la définition du traitement. Celui-ci vise « toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction »[20].

Constitue donc un traitement de données toute action réalisée sur celles-ci, de la collecte à l'effacement. En matière procédurale, la collecte de données renvoie notamment au recueil de

[16] Art. 6 de la loi informatique et libertés.
[17] *Ibid*.
[18] Art. 5 de la loi informatique et libertés dans sa rédaction initiale.
[19] Art. 2 de la directive du 24 octobre 1995. Ces termes sont ensuite repris à l'article 2 de la loi informatique et libertés suite à sa modification par la loi du 6 août 2004.
[20] Art. 4 du règlement général sur la protection des données.

preuves et d'informations sur les différents acteurs de la procédure. Toutes les données nécessaires au bon déroulement d'une procédure judiciaire comportent évidemment des données personnelles au sens de la loi.

5. Le cadre des procédures judiciaires – Le terme de procédure se définit comme « l'ensemble de règles régissant le déroulement du procès »[21]. Si l'on observe l'étymologie du terme « judiciaire » celui-ci renvoie au terme latin *judiciarius* (relatif à la justice) et *judico* (juger), visant donc l'action de juger. Par opposition à la justice administrative, le terme de judiciaire peut être attaché à ce « qui concerne la justice rendue par les tribunaux judicaires »[22], placés sous l'autorité de la Cour de cassation. Ainsi, la procédure judiciaire renvoie aux règles de droit processuel qui encadrent le déroulement du procès civil ou pénal. En matière pénale, la procédure désigne « l'ensemble des règles d'organisation judiciaire et de conduite d'une instance aboutissant, à partir de l'élaboration d'un dossier de procédure, à un jugement définitif »[23]. Toutefois, la procédure peut ne pas aboutir au procès et s'arrêter avant que la juridiction de jugement ne soit saisie, par la mise en œuvre de procédures alternatives par exemple[24].

Ainsi, traditionnellement, la procédure pénale englobe les règles applicables à la constation des infractions, l'identification des auteurs, la poursuite et le jugement. Conservant cette approche classique, ne sera pas abordée la question des données traitées dans la phase post-sentencielle d'application des peines. De la même manière la procédure civile s'entend des actes nécessaires, de la mise en état d'une affaire au jugement rendu[25]. Sera donc exclue de ces travaux la phase d'exécution des décisions.

De plus, le sujet visant les données traitées au cours de procédures judiciaires, la question des modes de règlement amiables des différends ne sera pas abordée[26]. Ces modes de règlement des litiges en dehors du juge peuvent prendre aujourd'hui de nouvelles formes avec la création des services de médiation et conciliation en ligne. Ces nouveaux services intéressent néanmoins la question du traitement de données personnelles notamment parce qu'ils reposent sur l'utilisation de plateformes d'échange de données pouvant le cas échéant être sensibles. La loi de programmation du 23 mars 2019 est venue apporter des précisions en la matière dans le

[21] R. Cabrillac, *Dictionnaire de vocabulaire juridique*, LexisNexis, 12e ed., 2021.
[22] G. Cornu, *Vocabulaire juridique*, PUF, 13e ed., 2020.
[23] S. Guinchard, J. Buisson, Procédure pénale, LexisNexis, 12e ed., 2019, p. 2.
[24] *Ibid*.
[25] Voir, S. Guinchard, F. Ferrand, C. Chainais, L. Mayer, Procédure civile, Dalloz, 6ème ed., 2019.
[26] Voir sur le sujet, L. Benraïs, C. Butruille-Cardew, N. Fricero, B. Gorchs-GelzerG. Payan, *Le guide des modes amiable de résolution des différends*, Dalloz, 3e éd., 2017/2018.

but affirmé de développer le recours à ces modes alternatifs[27]. Ainsi, la loi précise que les personnes physiques ou morales mettant à disposition un service de médiation de conciliation ou d'arbitrage en ligne sont soumises aux obligations relatives à la protection des données et à la confidentialité de celles-ci[28]. De plus, ces services ne peuvent reposer sur un seul traitement automatique ou algorithmique de données[29].

6. Le traitement de données à caractère personnel : un sujet étendu – L'étude du sujet implique nécessairement d'en fixer les contours. De cette évidence découle la première difficulté attachée à ces travaux. Le premier constat est celui d'un sujet vaste aux termes larges. En effet, le terme de données à caractère personnel renvoie en réalité à une multitude d'informations. De la même manière, le traitement de ces données peut prendre des formes variées. La difficulté de l'étude réside dans le fait que le traitement de données à caractère personnel dans les procédures judiciaires renvoie à une multitude de notions diffuses face à des problématiques et un cadre qui se veulent mouvants. Il s'agit donc de s'intéresser aux données identifiantes, même indirectement, qui interviennent au cours d'une procédure judiciaire, par le biais d'un traitement automatisé ou non visant la collecte, la conservation, l'utilisation, le transfert, la rectification, l'effacement de celles-ci.

Les problématiques attachées au traitement des données personnelles ne sont pas nouvelles mais force est de constater que ces dernières années ont été marquées par un engouement certain pour la matière sans nul doute lié au développement d'internet et du *big data*. Ce contexte et les risques qui en découlent ont conduit à repenser les normes encadrant le traitement des données personnelles.

7. Les normes spécifiques à la matière – La Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, signée le 28 janvier 1981 et ratifiée par la France le 24 mars 1983 dite « Convention 108 » est venue apporter des garanties quant au traitement des données personnelles notamment s'agissant des flux transfrontaliers. Elle définit les principes nécessaires au traitement licite et loyal des données personnelles et pose les bases qui seront développées par la suite de finalité légitime du traitement, de nécessité du traitement, d'exactitude des données et de conservation limitée au temps nécessaire. De plus, la

[27] Loi n° 2019-222 du 23 mars 2019 de programmation2018-2022 et de réforme pour la justice.
[28] Art. 4 de la loi de programmation du 23 mars 2019.
[29] *Ibid.*

Convention 108 fait référence au droit pour l'individu concerné par un traitement d'avoir connaissance ou confirmation de celui-ci et le cas échéant d'obtenir rectification ou effacement des données. D'ores et déjà étaient prévues des exceptions quant aux données traitées pour des raisons de sécurité publique ou de répression des infractions pénales.

Face aux développements technologiques entrainant des flux de plus en plus importants de données entre les Etats, la directive européenne du 24 octobre 1995 a eu pour vocation de garantir un niveau de protection des données sur tout le territoire de l'Union du fait notamment des différences en termes de droits et libertés qui existent entre ces Etats et qui constituent un obstacle à l'échange de données entre eux. Néanmoins il faut noter la transposition tardive de la directive en France par une loi du 6 août 2004.

Le règlement général sur la protection des données adopté en 2016[30] est venu adapter les normes existant en la matière pour les mettre en adéquation avec les évolutions en termes de technologies et de modes de communication. Le règlement rappelle que la protection des personnes physiques eu égard au traitement de leurs données personnelles est un droit fondamental[31], ce droit n'est pour autant pas absolu[32] et nécessite une mise en balance avec les autres droits fondamentaux auxquels il se confronte. Face aux évolutions technologiques et économiques qui ont entrainé des flux de données entre Etats, et aux risques engendrés par ces flux massifs de données, le règlement a vocation à garantir au sein de tous les Etats un niveau de protection élevé, visant un cadre « solide et plus cohérent »[33]. C'est aussi pour pallier aux faiblesses de la directive du 24 octobre 1995 que le règlement entend mettre en œuvre une homogénéisation des seuils de protection permettant de faciliter le transfert de données entre Etats là où les différences de régimes créaient des obstacles[34]. S'agissant des traitements mis en œuvre par les autorités dans l'exercice de leurs missions, le règlement autorise et invite les Etats membres à préciser les normes applicables notamment en matière de traitement de données sensibles[35]. Cette protection renforcée nécessitait de renforcer également les droits des individus quant à leurs données personnelles et en parallèle d'accentuer la surveillance et la mise en place de contrôle effectifs sur les traitements existants.

[30] 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).
[31] Cons. 1er du règlement général sur la protection des données.
[32] *ibid*. cons. 4.
[33] *ibid*. cons. 7et 10.
[34] *ibid*. cons. 9.
[35] *ibid*. cons. 10.

8. L'affirmation du principe de gouvernance interne « Accountability » par le règlement général sur la protection des données – L'adoption du règlement général sur la protection des données marque une évolution majeure dans le droit de la protection des données à caractère personnel en mettant un terme au système d'autorisation préalable à la mise en œuvre d'un traitement autrefois dévolue à la Commission nationale de l'informatique et des libertés (CNIL). Le réglement supprime ce contrôle *a priori* sur les traitements et réaffirme et accentue les obligations des responsables de traitements. Le traitement des données se trouve donc régie par les mécanismes de gouvernance interne désignés sous le vocable *d'accountability*[36]. Basée sur la responsabilisation des personnes mettant en œuvre un traitement de données, le système de protection mis en œuvre par le règlement général développe, plus que les textes antérieurs, les obligations qui incombent au responsable du traitement en termes notamment de sécurité des données. Ainsi, l'article 5 du règlement général s'il pose les principes devant être observés pour tout traitement, précise bien qu'il revient au responsable de s'assurer de leur application. Ces dispositions sont reprises à l'article 121 de la loi informatique et libertés qui dispose que « le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès ».

Le règlement général sur la protection de données renforce des mesures préexistantes, en fixant des « mesures organisationnelles », en imposant des « mesures de protection » et en renforçant les sanctions attachées au non respect de ces règles[37]. L'article 24 du règlement général vise l'obligation pour le responsable du traitement de mettre en œuvre des « mesures techniques et organisationnelles ».

S'agissant des mesures organisationnelles, celles-ci prennent la forme par exemple de l'obligation de tenir un registre des activités, mis à disposition de la CNIL, qui contient des informations relatives à la finalité du traitement, aux données concernées ainsi qu'à l'identité du responsable[38]. Le règlement général pose l'obligation de désigner un délégué à la

[36] N. Metallinos, Le principe d'accountability des formalités préalables aux études d'impact sur la vie privée, *Communication commerce électronique*, n°4, avril 2018 , doss. 11.

[37] Reprenant ici la présentation faite par C. Féral-Schuhl dans son ouvrage. *Cyberdoit*, Le droit à l'épreuve de l'internet, Dalloz, 8e ed., 2020/2021.

[38] Art. 30 du règlement général sur la protection des données, Art. 57 de la loi informatique et libertés.

protection des données chargé de veiller au respect de la réglementation[39]. Toutefois, cette obligation ne concerne pas les juridictions[40].

S'agissant des mesures de protection[41], le règlement général prévoit la réalisation d'une analyse d'impact lorsque le traitement est susceptible de porter atteinte aux droits et libertés des individus notamment, lorsqu'il porte sur des données sensibles au sens de l'article 9 ou vise des données pénales[42]. Cette protection passe aussi par l'obligation pour le responsable du traitement de respecter les principes encadrant le traitement de données. Il s'agit ici du *privacy by default,* qui garantie le principe de finalité des données qui ne sont utilisées que par nécessité, le temps de conservation ne devant pas excéder le temps nécessaire à cette finalité. Aussi, le terme de *privacy by design* renvoie aux principes visant la protection des données dès leur mise en œuvre.

Enfin, les nouvelles dispositions sanctionnent plus sévèrement le non respect des normes encadrant le traitement de données. Cela passe dans un premier temps par la dotation de nouveaux moyens à la CNIL qui peut prononcer de nouvelles sanctions[43] qui viennent s'ajouter aux dispositions du code pénal[44].

9. Les principes encadrant le traitement de données à caractère personnel – Le traitement de données à caractère personnel doit répondre à certains principes. Il doit être licite, loyal et transparent[45]. Le traitement doit répondre à une finalité déterminée et la collecte être pertinente et adéquate au vu de ces finalités. Les données collectées doivent être exactes, mises à jour et conservées le temps nécessaire. Enfin elles doivent être traitées de manière sécurisée. La licéité repose soit sur le consentement de l'intéressée, soit sur un motif déterminé par les textes. Par exemple il peut s'agir de traitements nécessaires aux autorités publiques dans l'exercice de leurs missions, ou nécessaires à l'exécution d'une mission d'intérêt public[46].

[39] G. Desgens-Pasanau, Le délégué à la protection des données, pierre angulaire du principe de responsabilité, *Communication commerce électronique*, n°4, avril 2018, doss. 6.
[40] RGPD art. LIL art. 57.
[41] C. Féral-Schuhl, *Cyberdoit*, *Le droit à l'épreuve de l'internet*, *op. cit.* p. 1096 et s.
[42] Art. 35 du règlement général sur la protection des données et art. 62 de la loi informatique et libertés. C. Féral-Schuhl, *Cyberdoit, Le droit à l'épreuve de l'internet*, *op. cit.* p. 1096 et s.
[43] Art. 20 et s. de la loi informatique et libertés.
[44] Art. 226-17 et s. du code pénal.
[45] Art. 4 de la loi informatique et libertés.
[46] Art. 5 de la loi informatique et libertés.

10. Dispositions propres aux données pénales – S'agissant des données intervenant en matière de prévention et détection des infractions, la directive du 27 avril 2016 dite « Police-Justice »[47] est venue encadrer leur traitement. Ces dispositions ont vocation à fixer des normes encadrant le traitement de données personnelles adaptées et conciliables avec le bon déroulement de la justice qui nécessite des traitements de données parfois intrusifs et la mise en œuvre de procédés de collecte parfois coercitifs. Les principes qui s'appliquent prennent notamment en considération la nature et la gravité de l'infraction à l'origine du traitement. Cette directive constitue avec le règlement général le « paquet européen » qui a été transposé en droit interne dans la loi informatique et libertés aux articles 87 et suivants.

11. Les enjeux modernes du traitement de données – Les évolution de la société qu'elles soient technologiques, scientifiques ou simplement sociétales, ont modifié la définition même du traitement de données à caractère personnel et les enjeux de ces traitements. Il est évident que cela a contribué à l'évolution des normes encadrant la matière. Ces évolutions ont entrainé l'obsolescence des lois régissant le traitement de données.

Parmi ces évolutions, il faut mentionner les évolutions scientifiques et les progrès de la génétique qui a eu un impact important tant en matière civile que pénale, permettant d'un coté l'établissement du lien de filiation et de l'autre l'identification d'individus et notamment d'auteurs d'infractions. Depuis les années 50, avec la découverte de la structure de l'ADN, la science a développé de nouveaux procédés d'analyse qui permettent désormais d'établir le profil génétique d'un individu à partir d'une quantité infime de matière[48]. En termes de procédure judiciaire, le recours à l'ADN suppose la collecte et la conservation de données sensibles.

Les nouvelles technologies ont également entrainé l'évolution des modes de communication. Le développement d'internet et des échanges dématérialisés ont poussé à repenser le traitement de données. Les textes ont du s'adapter à l'usage de la donnée numérique, leur collecte soulevant des interrogations nouvelles ainsi que leur utilisation comme preuve. La reconnaissance de l'écrit numérique marque l'admission de ce nouveau mode de communication. Néanmoins dans la reconnaissance de cette preuve numérique peut justement

[47] 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, et abrogeant la décision-cadre 2008/977/JAI du Conseil.

[48] Voir, M. Schwendener, *Police technique et scientifique*, Répertoire de droit pénal et de procédure pénale, octobre 2016 actualisation février 2019.

se poser la question de la force probante de la preuve électronique orale qui nécessite une certaine fiabilité[49]. Les procédures judiciaires n'échappent pas à la dématérialisation des échanges comme en témoignent les récents textes qui marquent une avancée dans la mise en œuvre de la dématérialisation des procédures[50].

Le droit des données à caractère personnel a dû s'adapter à la fois aux nouveaux modes de communication et d'échange de données, échanges qui visent un nombre croissant de données qui touchent pour certaines à l'identité directe des individus tels que les données biométriques. Le développement d'internet et de l'information de manière générale permet quoi qu'il en soit une identification des individus par recoupement de données quand bien même l'information divulguée serait limitée.

12. La protection des données à caractère personnel et le droit au respect de la vie privée – Le droit de la protection des données à caractère personnel est sans nul doute empreint d'une grande transversalité. Celle-ci se retrouve dans l'expression qui a pu être posée de « droit de la donnée »[51]. Néanmoins, les références divergent, parfois elles visent le droit de la protection des données, parfois le droit à la protection des données soulevant la question de l'autonomie de ce droit et sa consécration comme droit subjectif.

La Charte des droits fondamentaux vise en son article 2 le droit à la protection des données à caractère personnel. Celles-ci devant être traitées de manière loyale et reposer sur le consentement ou sur fondement prévu par la loi. Ces dispositions sont reprises à l'article 16 du traité sur le fonctionnement de l'Union européenne.

Il ne fait nul doute que la notion de vie privée et celle de données à caractère personnel se rapprochent en ce qu'elles sont attachées à la notion d'identité, néanmoins elles ne se confondent pas[52].

L'article 1er de la loi informatique et libertés dispose d'ailleurs que « l'informatique doit être au service de chaque citoyen. Son développement doit s'opérer dans le cadre de la coopération internationale. Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques ».

La notion de données personnelle renvoie aux informations qui permettent l'identification des individus. Cette identificabilité nécessite d'encadrer le traitement de ces données. Les textes

[49] A. Lecourt, Procédure civile et numérique, *Dalloz IP/IT et communication*, juin 2020.
[50] Notamment le Décret n° 2005-1678 du 28 décembre 2005 , le décret n° 2019-302 du 3 mai 2019.
[51] M. Bourgeois, *Droit de la donnée. Principes théoriques et approche pratique*, LexisNexis, 2019. De par cette transversalité et « omniprésence » l'auteur préfère l'expression « droit de la donnée » à celle de « droit des données ».
[52] C. Féral-Schuhl, *Cyberdoit*, *Le droit à l'épreuve de l'internet*, *op. cit.* p. 111.132

adoptés en la matière tendent finalement à consacrer des obligations pour les responsables et à affirmer des droits pour les individus visés, comme notamment le droit d'accès, de rectification, d'opposition ou d'effacement. Ainsi, un traitement qui ne serait pas ou plus nécessaire n'a plus lieu d'être et doit donner droit à l'effacement des données qu'il contient. Aussi, le règlement général sur la protection des données consacre un droit au déréférencement en matière de données mises en ligne. En cela, les textes semblent consacrer un droit de regard et d'action aux individus sur les traitements de données les concernant. Ce qui amène davantage à la conclusion de l'existence d'un droit à l'autodétermination informationnelle[53]. Les atteintes aux données personnelles sont attachées au non respect des normes encadrant leur collecte et leur utilisation. Le droit au respect de la vie privée consacré dans les textes[54] se définit par rapport à l'atteinte subie par la personne. On citera la notion telle que retenue par le doyen Carbonnier qui définit la vie privée comme « une sphère secrète de vie où l'individu aura le pouvoir d'écarter les tiers »[55]. La vie privée a pu être présentée comme étant « prioritairement un droit à l'anonymat. Toute identification de la personne, sans son consentement, par quelque moyen que ce soit, nom, numéro, image, voix… est constitutive d'une atteinte à la vie privée ouvrant droit à réparation à raison de cette seule atteinte »[56].

L'article 9 du code civil pose le droit au respect de la vie privée. Par ailleurs, les articles 226-1 et suivants du code pénal sanctionnent les atteintes faites à la vie privée. Ils visent le fait de volontairement y porter atteinte par notamment la captation ou la transmission d'image sans le consentement de l'intéressé, la conservation ou la diffusion publique de ces données. Le code pénal vise à ce titre toute atteinte volontaire à l'intimité, la violation du domicile. Les incriminations attachées au traitement de données personnelles sont prévues aux articles 226-16 et suivants du code pénal qui visent le non respect des règles de licéité dans la mise en œuvre du traitement.

La notion de données à caractère personnel apparait donc plus large que celle de vie privée, plus large par rapport aux informations visées mais plus restreinte dans son application. Une atteinte à la protection des données personnelles peut éventuellement porter atteinte au droit au respect de la vie privée. En cela, le droit au respect de la vie privée permet de sanctionner les atteintes à celle-ci alors que le droit de la protection des données à caractère personnel permet la sanction du non respect des normes relatives au traitement. Les deux notions sont

[53] P. Türk, L'autodétermination informationnelle : un droit fondamental émergent ?, *Dalloz IP/IT*, 2020, 616.
[54] Art. 9 du code civil, art. 8 de la Conv. E.D.H.
[55] J. Carbonnier, *Droit civil : Les personnes*, t. I, 20e éd., 1996, no 86.
[56] J.C. Saint-Pau, *L'anonymat et le droit*, thèse, Bordeaux IV, 1998.

foncièrement liées car elles touchent à l'identité des individus, et apparaissent donc davantage complémentaires que concurrentes[57].

13. Les problématiques soulevées par le traitement de données à caractère personnel dans les procédures judiciaires – Le sujet appelle une présentation chronologique permettant d'appréhender les différentes problématiques soulevées par le traitement de données à caractère personnel dans le cadre des procédures judiciaires. Le traitement visant toute action effectuée sur la donnée de sa collecte à son effacement, ces différentes actions sur la donnée seront abordées en suivant la chronologie de la procédure.

Ainsi il convient dans un premier temps de s'intéresser à la collecte de données personnelles en tant que recueil de données probatoires, soulevant des interrogations relatives à l'administration de la preuve, la légalité et la loyauté dans les procédés utilisés. Les évolutions technologiques ont permis l'émergence de nouveaux modes de preuves qui soulèvent pour certains des interrogations attachées notamment au caractère intrusif des procédés de recueil comme s'agissant du recueil ADN par exemple. Aussi, le développement d'internet a conduit à adapter les normes en matière de preuve avec notamment la reconnaissance de l'écrit numérique. Cette dématérialisation des échanges et le développement du *big data* ont à la fois permis la création de nouveaux mode d'enquête[58] mais aussi ont entrainé le développement de nouvelles formes de délinquance et de criminalité.

Les données collectées font l'objet d'un nécessaire fichage. Cette mémoire judiciaire permet la conservation de données à vocation probatoires utiles à la résolution de litiges avec parfois une utilité différée dans le temps. Le recueil de traces ou de données biométriques permet par interrogation d'autres fichiers l'identification d'auteurs d'infractions. En cela, le fichage de données biométriques a constitué une avancée considérable dans en matière d'identification. Si l'on ne peut nier les avancées permises par de tels fichages, ces derniers interrogent et inquiètent. Les controverses sont légitimes et soulèvent la question de la collecte massive de données personnelles au sein de fichiers qui se veulent de plus en plus nombreux et de plus en plus importants de par le nombre de données conservées et de par le nombre des personnes visées. Le fichage de données doit rester attaché au critère de nécessité et de proportionnalité et impose donc un contrôle strict afin de ne pas déborder abusivement sur les droits et libertés des individus. En cela, l'établissement d'un cadre strict relatif à la création de tels traitements,

[57] Par exemple, la conservation de données personnelles réalisée sans le consentement de l'individu et sans base légale constitue une atteinte au droit au respect de la vie privée sur le fondement de l'article 226-1 du code pénal et constitue également une atteinte à la protection des données au sens de l'article 226-17 du code pénal.

[58] B. Roussel, *Les investigations numériques en procédure pénale*, Thèse, Bordeaux, 2020.

l'existence de contrôles effectifs sur ces derniers et l'affirmation de droits pour les individus concernés semblent nécessaires.

Ensuite, se pose les questions attachées à la communication de ces données au cours de la procédure que se soit par l'application des principes directeurs du procès ou par l'application du droit à l'information. Le traitement de données dans ce contexte procédural soulève également des interrogations quant à la mise en œuvre des principes de droit processuel qui impliquent la diffusion de données au nom de l'application des principes de publicité ou du contradictoire qui trouvent à se poser tant en matière pénale que civile. Certaines données de par leur nature bénéficient d'une protection particulière, la question de l'accès et de la divulgation de données secrètes trouve alors particulièrement à se poser, notamment s'agissant du secret de l'enquête et de l'instruction et plus généralement des données relevant d'un secret professionnel. Le développement des modes de communication et l'aspiration à une transparence toujours grandissante conduisent à s'interroger sur la diffusion des données judiciaires sur internet et dans la presse[59]. L'équilibre est alors délicat à trouver entre la liberté d'expression et le secret de l'enquête et de l'instruction nécessaire au bon déroulement de celles-ci.

Au delà, il faut s'interroger sur la question de la mise en open data des décisions de justice notamment depuis l'adoption des textes récents en la matière. Cette diffusion massive de données sur internet notamment, interroge sur l'existence d'un droit à l'oubli sur des données qui deviennent difficilement traçables sur internet. Cela soulève la question de la place de l'oubli dans une société qui aspire de plus en plus au souvenir et à la transparence. Cette évolution a nécessité d'adapter les normes applicables avec la consécration notamment d'un droit au déréférencement qui connait néanmoins des limites. De la même manière, les garanties découlant des procédés d'occultation des données identifiantes connait des limites. Enfin se pose la question du sort des données qui ont été collectées au cours d'une procédure soulevant ici des interrogations en terme de gestion des données fichées et d'effacement de celles-ci, ce qui renvoie nécessairement à la question de l'oubli en rapport avec la mémoire judiciaire et la mémoire collective.

Face aux évolutions tant technologiques que scientifiques qui ont un impact certain sur le traitement des données intervenant dans les procédures, il convient d'analyser comment sont encadrés ces différents traitements afin de garantir la protection des données concernées et le respect des droits des individus. Cette problématique impose un raisonnement en deux temps.

[59] E. Netter, A quoi sert le principe de transparence en droit des données personnelles ? *Dalloz IP/IT*, 2020, 611.

Le premier est destiné à l'étude des traitements mis en œuvre et qui permettent l'exploitation des données à caractère personnel dans les procédures judiciaires, le second analysant la manière dont les données sont protégées durant cette procédure.

Il convient donc de s'intéresser dans un premier temps à l'exploitation des données à caractère personnel dans les procédures judiciaires (Partie 1), puis dans un second temps à la protection des données à caractère personnel dans les procédures judiciaires (Partie 2).

PREMIERE PARTIE
L'EXPLOITATION DES DONNEES A CARACTERE PERSONNEL DANS LES PROCEDURES JUDICIAIRES

14. Les données à caractère personnel constitutives de données probatoires – Le traitement des données à caractère personnel renvoie en ce qui concerne les procédures judiciaires aux questions attachées à la collecte de données probatoires. Cette collecte vise le recueil de preuves qui peut, classiquement, s'analyser sous l'angle de l'administration de la preuve et de son appréciation. Au regard de la définition large attribuée aux données à caractère personnel[60], il apparait comme une évidence que ces dernières constituent potentiellement des données probatoires dans les procédures judiciaires. Ces données attachées à l'identité des personnes peuvent constituer des éléments d'identification et notamment permettre d'apporter la preuve de la participation d'un individu à la commission d'une infraction, pour ce qui est de la matière pénale. Aussi pour ne donner qu'un exemple, ces données peuvent intervenir afin de prouver l'existence d'un préjudice avec notamment l'utilisation de données médicales dans le procès civil. Il ne s'agit donc pas ici de faire la démonstration de la nécessité d'user de données à caractère personnel en tant que données à vocation probatoire dans le procès, mais plutôt d'observer les procédés de collecte de ces données et d'analyser leur valeur probatoire au regard des normes encadrant le recueil de preuve et au regard des dispositions adoptées en matière de protection des données.

15. Traitements variés de données à caractère personnel à vocation probatoire – Les données à caractère personnel exploitées au cours de procédures judiciaires sont collectées par le biais de différents procédés, utilisés tant par les autorités publiques que par les particuliers, qui doivent répondre à une exigence de licéité. Cette notion de licéité renvoie à la légalité dans la collecte de preuve et au principe de loyauté[61]. Ces deux aspects amènent à s'interroger de manière générale sur l'application qui est faite des principes encadrant l'administration de la preuve et de manière plus particulière sur le traitement des données à caractère personnel telles que visées par les textes en matière de protection de données. Aussi, se pose la question des modes de recueil en fonction de la nature des données qui peuvent constituer des données sensibles ou protégées.

[60] V. *supra* n°2.
[61] E. Vergès, G. Vial, O. Leclerc, *Droit de la preuve*, PUF, 2015.

Le traitement tel que défini par le règlement général sur la protection des données et la loi informatique et libertés vise également le stockage des données collectées. S'agissant des données à caractère personnel intervenant dans les procédures judiciaires ce stockage se traduit par la constitution et l'alimentation de fichiers judiciaires qui soulèvent, là encore, des interrogations multiples tant en termes de nécessité du fichage que de finalité du traitement et de sécurité des données fichées.

16. Evolutions dans le traitement de données en matière judiciaire – Plusieurs constats s'imposent s'agissant du traitement de données judiciaires. Premièrement s'agissant de la collecte de données probatoires, on assiste à un développement des procédés de recueil et au-delà à une extension de l'application des procédés existants. Les développements technologiques ont permis de faciliter le recueil de preuves et d'exploiter de nouvelles preuves. Par exemple, les progrès en matière de génétique marquent une évolution majeure dans le système probatoire.

Le deuxième constat est que le droit de la preuve a du s'adapter aux évolutions de la société. Avec notamment l'avènement d'internet, il a fallu repenser les normes encadrant le droit de la preuve avec à la fois l'émergence de nouveaux modes de preuve mais aussi, en parallèle, l'émergence de nouvelles formes de criminalité comme la cybercriminalité par exemple. En cela, internet apparait à la fois comme un nouveau moyen d'action et comme une nouvelle menace.

Enfin, on a assiste à un stockage de plus en plus massif de données à caractère personnel au sein de fichiers judiciaires, conséquence des nouveaux modes de recueil mais aussi des lois augmentant les faits justifiant le fichage.

17. Problématiques – Des interrogations se posent quant aux procédés de collecte utilisés au regard des principes du droit de la preuve mais aussi au regard de la nature des données concernées. De la même manière, le stockage de données soulève la question de la nécessité d'un tel fichage et celle de la protection des données fichées.

Il convient donc de s'intéresser aux données à caractère personnel intervenant dans les procédures judiciaires à titre probatoire (Titre 1er), données à caractère personnel alimentant des fichiers judiciaires (Titre 2).

TITRE PREMIER
LES DONNEES A CARACTERE PERSONNEL INTERVENANT DANS LES PROCEDURES JUDICIAIRES A TITRE PROBATOIRE

18. Le droit de la preuve sous l'angle du droit de la donnée – L'intérêt du sujet est de s'interroger sur les normes encadrant la collecte de données en adoptant un regard guidé par le droit de la preuve et les règles régissant le traitement de données à caractère personnel. Le recueil de preuves s'analyse en une collecte de données à caractère personnel et constitue évidemment un traitement de données au sens de la loi informatique et libertés et du règlement général sur la protection des données. L'idée est donc de s'intéresser à la collecte de données à caractère personnel constitutives de preuves potentielles dans une procédure judiciaire en s'interrogeant sur l'application des principes de loyauté et de légalité. Ce préalable nécessaire permet ensuite de s'interroger plus spécifiquement sur l'impact de la nature des données collectées sur le recueil de preuves. De manière générale, le droit processuel et le droit de la preuve soulèvent des questions relatives au recueil de preuves et à l'appréciation de leur valeur probante. Raisonnant d'un point de vue des données à caractère personnel, les mêmes dispositions trouvent à s'appliquer mais il convient d'y porter un regard particulier et d'appréhender ces questions sous l'angle des dispositions propres aux données à caractère personnel en ce qu'elles constituent d'éventuelles preuves dans le procès.

19. Les conséquences de l'émergence de nouvelles formes de criminalité – En matière pénale, l'émergence de nouvelles formes de criminalité a poussé le législateur à développer de nouveaux procédés de recueil de preuves dans le but notamment de garantir une meilleure lutte contre les infractions. Ces nouvelles procédures touchent notamment aux domaines scientifiques et numériques qui par nature supposent de traiter des données à caractère personnel sensibles. Pour cette raison, le recueil de preuves scientifiques tels que l'ADN ou les données biométriques et le recueil de données numériques soulèvent des interrogations propres à la nature même des preuves que constituent ces données à caractère personnel sensibles. De manière générale, les données à caractère personnel exploitées lors de procédures judiciaires sont à appréhender comme de potentiels outils probatoires dans le procès. Ces données sont donc soumises aux règles qui régissent l'appréciation de la preuve qu'elle soit légale ou libre. Toutefois, la question de la hiérarchie des preuves soulève des

problématiques particulières s'agissant de certains types de données. Si en principe, le juge est libre d'apprécier la valeur des preuves présentes dans le dossier de la procédure, les données scientifiques ou numériques semblent parfois bénéficier d'une autorité supérieure, ce qui induit certaines interrogations. Face au développement de ce type de preuves, le législateur a du adapter certaines dispositions de la loi. La jurisprudence et la doctrine apportent sur la question des enseignements et des réflexions utiles démontrant parfois la nécessaire évolution du droit face au traitement de données à caractère personnel.

20. La libre admissibilité des modes de preuve – En droit civil, le principe de liberté de la preuve a été inscrit à l'article 1358 du code civil par l'ordonnance du 10 février 2016[62]. L'ordonnance a repris des règles applicables antérieurement et fait de la liberté de la preuve le principe en exposant ensuite les exceptions. En vertu des dispositions de l'article 1358 du code civil, les faits juridiques peuvent être prouvés par tout moyen. Ceci renvoie donc à un grand nombre de moyens tels que les écrits ou les témoignages. L'article 1363 du code civil dispose désormais expressément que *« nul ne peut se constituer de titre à soi-même »*. Le législateur renvoie donc ici à la preuve des actes juridiques et affirme le principe admis par la jurisprudence selon lequel la preuve autoconstituée est possible s'agissant des faits juridiques[63].

En droit pénal, la preuve peut également se faire par tout moyen. L'objectif étant ici de prouver qu'une infraction a été commise et d'identifier son auteur. Le principe de liberté de la preuve se retrouve à l'article 427 du code de procédure pénale[64]. Ce principe est admis en matière délictuelle et criminelle, seule la matière contraventionnelle est soumise au principe de la preuve légale. Ainsi, les modes de preuve admissibles sont l'aveu, l'indice, la preuve littérale et le témoignage, qui peuvent pour certains soulever des interrogations particulières en termes de droit des données

21. Intérêt du sujet – Partant de l'évidence selon laquelle le recueil de preuves entraine une collecte de données au sens de la loi informatique et libertés, l'intérêt du sujet est d'observer et d'analyser les normes qui encadrent l'administration de la preuve en adoptant si possible

[62] Ordonnance n° 2016-131 du 10 février 2016 portant réforme du droit des contrats, du régime général et de la preuve des obligations.
[63] Cass. civ. 2e, 6 mars 2014, *pourvoi* n°14-14.295, *inédit.* Cass. civ. 1ère, 1er octobre 2014, *pourvoi* n °13-24.699.
[64] Art. 427 du code de procédure pénale *« Hors les cas où la loi en dispose autrement, les infractions peuvent être établies par tout mode de preuve et le juge décide d'après son intime conviction. Le juge ne peut fonder sa décision que sur des preuves qui lui sont apportées au cours des débats et contradictoirement discutées devant lui. »*

une approche sous l'angle du traitement de données. Il convient de s'intéresser dans un premier temps à la collecte de données à caractère personnel au regard des principes encadrant la licéité de la preuve (Chap. 1). Partant de cette présentation traditionnelle, il convient ensuite de s'interroger sur l'impact de la nature particulière de données à caractère personnel sur leur fonction probatoire (Chap. 2).

CHAPITRE 1 : LA COLLECTE DE DONNEES A CARACTERE PERSONNEL AU REGARD DES PRINCIPES ENCADRANT LA LICEITE DE LA PREUVE

22. La collecte de données à caractère personnel soumise au principe de licéité de la preuve – S'agissant des données à caractère personnel, l'article 5 de la loi informatique et libertés précise les conditions de licéité du traitement. Ainsi, ce dernier doit se faire avec le consentement de l'intéressé, ou être nécessaire à l'exécution d'un contrat, au respect d'une obligation, à la sauvegarde des intérêts vitaux de la personne concernée, à l'exécution d'une mission d'intérêt public ou aux fins d'intérêt légitimes[65]. Cette condition d'intérêt légitime pourrait donc trouver sa source dans la nécessité de produire des données probatoires en justice. Le droit de la preuve soumet l'administration de celle-ci aux exigences de légalité[66]. Toutefois, la jurisprudence civile et pénale a dégagée un principe de loyauté dans l'administration de la preuve qui vient compléter l'exigence de légalité. Cette loyauté qui n'est pas consacrée par les textes demeure toutefois incertaine dans sa portée. Si la jurisprudence l'a érigé en principe directeur du procès, l'absence d'inscription dans les textes et le rejet d'une telle inscription témoignent de sa complexité. Tant la doctrine que certaines décisions amènent une certaine confusion. Avec parfois des références plus générales à la licéité, ou alors des raisonnements sur le fondement de la vie privée, il peut être compliqué de définir les contours de la loyauté de la preuve[67]. On remarque notamment parfois une certaine confusion entre la « légalité matérielle »[68] et la loyauté de la preuve, certains voyant en la

[65] Art. 5 de la loi informatique et libertés « 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. »
[66] E. Vergès, G. Vial, O. Leclerc, *Droit de la preuve, op. cit.*
[67] J.H. Robert, Le principe de loyauté dans la recherche de la preuve dans le procès civil et pénal, Actualités du droit civil, Lamy, 2 aout 2019.
[68] V. *infra* n°59 s.

loyauté une application du principe de légalité matérielle[69]. Aussi une autre difficulté tient dans le fait que le principe connait une application différente en fonction de la nature du contentieux, que celui-ci dépende des juridictions civiles ou pénales.

Cette double exigence de légalité et de loyauté est qualifiée par la doctrine contemporaine sous le terme de licéité de la preuve[70]. La donnée à caractère personnelle collectée à des fins probatoires dans une procédure est *de facto* soumise à cette double exigence.

Il convient dont de s'intéresser à la collecte de données à vocation probatoire soumise au principe de légalité de la preuve (Section 1) puis à la collecte de données à vocation probatoire soumise au principe de loyauté de la preuve (Section 2).

Section 1 : La collecte de données à vocation probatoire soumise au principe de légalité de la preuve

23. Etendue du principe de légalité – Le principe de légalité renvoie à la fois aux obstacles à la preuve tels que le respect de la vie privée, la dignité ou encore aux règles particulières qui encadrent certains procédés, notamment en matière pénale. La légalité de la preuve est invoquée au fondement de demandes d'annulation d'actes. Il convient de distinguer la légalité « matérielle » de la légalité « formelle »[71]. La légalité « matérielle » vise des principes généraux du droit qui prohibent, par exemple, tout procédé de recueil de preuve qui porterait atteinte au droit au respect de la vie privée ou à la dignité des personnes et ce peu importe l'infraction commise[72]. La légalité « formelle » renvoie quant à elle à l'encadrement du recueil de preuve par la loi ce qui est particulièrement le cas en matière pénale notamment avec le développement de procédés de collecte de plus en plus intrusifs et coercitifs. C'est cette seconde approche qui intéresse particulièrement le sujet du traitement des données à caractère personnel.

La légalité de la preuve vise donc en premier lieu au cadre légal qui régit le recueil de preuves. La nécessité d'un tel cadre est d'autant plus évidente que les procédés de collecte peuvent être coercitifs.

---

[69] S. Guinchard, J. Buisson, *Procédure pénale*, *op. cit*, p. 472 et s.

[70] E. Vergès, G. Vial, O. Leclerc, *Droit de la preuve, op. cit.*

[71] Voir, J. Buisson, *Légalité de la preuve*, Répertoire de droit pénal et de procédure pénale, Dalloz, octobre 2020.

[72] La Cour européenne des droits de l'Homme dans l'arrêt du 18 janvier 1978, Irlande c/ Royaume-Uni (req. 5310/71) affirme que « le droit de ne pas subir un traitement contraire à la dignité de l'homme, parce qu'il est inhérent à la personne, pose une prohibition absolue, y compris au cas de lutte contre le terrorisme et le crime organisé ».Ce raisonnement est réaffirmé dans plusieurs arrêts : CEDH 18 octobre 2001, Indelicato c/ Italie, req. no 31143/96. CEDH, sect. V, 4 novembre 2010, *Darraj c/ France*, req. no 34588/07. CEDH, gr. ch., 11 juillet 2006, *Jalloh c/ Allemagne*, req.no 54810/00. CEDH 27 août 1992, *Tomasi c/ France*, req. No 12850/87.

Ensuite, la légalité invite à observer les normes qui peuvent constituer des obstacles dans la collecte de données probatoires, renvoyant ici notamment au respect de la vie privée ou à la dignité des individus. Le principe de légalité dans l'administration de la preuve invite à s'interroger dans un premier temps sur les textes qui encadrent les procédés de collecte puis ensuite de raisonner sur l'application faite du principe au regard des obstacles à la liberté de la preuve.

Il convient donc de s'intéresser à la collecte de données dans le respect de la légalité formelle (§1.), puis dans le respect de la légalité matérielle (§2.).

§1. Le respect de la légalité formelle

24. Portée du principe – La légalité dans le recueil de données probatoires renvoie aux dispositions légales qui encadrent certains procédés notamment en matière pénale. Tout acte d'administration de la preuve coercitif repose sur une base légale. Il s'agit de s'intéresser aux actes de collecte de données encadrés par la loi qui soulèvent des interrogations en termes de traitement de données à caractère personnel.

Au sein de la législation pénale, il est devenu classique de distinguer « le répertoire commun » [73] des actes, qui peuvent être réalisés par tout agent, du répertoire « spécial »[74] visant les actes de collecte relatifs à certaines infractions.

25. La collecte de données à caractère personnel encadrée – S'agissant de données à caractère personnel collectées en matière de prévention ou détection des infractions, le traitement est licite sur le fondement de l'exécution d'une mission d'intérêt public ou s'il est mis en œuvre par les autorités publiques dans l'exercice de leurs missions[75]. Si l'article 6 de la loi informatique et liberté prohibe, par principe, le traitement de toute donnée sensible comme par exemple les données biométriques permettant l'identification des individus, les autorités sont autorisées à traiter ces données. La licéité est alors attachée à la nécessité du traitement et doit reposer sur des dispositions légales et faire l'objet d'une étude d'impact préalable au vu des risques en termes de droit et libertés[76]. Il convient donc de s'intéresser à la réglementation générale des actes d'enquête (A.), puis à la collecte de données probatoires relevant de

[73] J. Buisson, *Preuve*, Répertoire de droit pénal et de procédure pénale, Dalloz, *op. cit.*
[74] *Ibid*.
[75] Art. 5 5° et 6° de la loi informatique et libertés.
[76] Art. 87 à 90 de la loi informatique et libertés.

procédés dérogatoires (B.) et enfin, à la collecte de données auprès des services de renseignement (C.).

A. La réglementation générale des actes d'enquête

26. Intérêt du sujet – Il ne s'agit pas ici de dresser la liste exhaustive des procédés de collecte de données probatoires mais plus de s'interroger sur certains d'entre eux présentant un intérêt particulier pour notre sujet.
Au vu des problématiques soulevées par le traitement de données à caractère personnel, on peut s'interroger sur les données collectées sur réquisition judiciaire (1°) par perquisition ou saisie (2°), ainsi qu'aux données interceptées (3°), aux données collectées par le recours aux expertises (4°) ainsi qu'à la collecte de preuves à l'étranger (5°).

1° Les données collectées sur réquisition judiciaire

27. Dispositions générales – L'officier de police judiciaire, le procureur de la République ou le juge d'instruction peuvent demander à ce que leur soient communiquées toutes informations ou documents utiles. Le secret professionnel ne peut, sauf motif légitime, faire obstacle à ces demandes. Ces mesures sont prévues aux articles 60-1 et 60-2 du code de procédure pénale s'agissant des enquêtes de flagrance, aux articles 77-1-1 et 77-1-2 du même code s'agissant des enquêtes préliminaires et enfin aux articles 99-3 et 99-4 s'agissant de l'instruction.
En application de ces dispositions, l'autorité en charge de l'enquête peut collecter toute donnée utile auprès de toute personne ou entité sans que le secret professionnel ne puisse lui être, par principe, opposé. Ces dispositions visent tout type de données peu importe leur support. La réquisition judiciaire constitue donc un mode de collecte de données qui ne connait que peu de limites et facilement mis en œuvre puisque justifié par les besoins de l'enquête d'accéder à ces données. Il s'agit ici d'une présentation brève puisque l'intérêt d'aborder cette question se trouve davantage dans l'étude des réquisitions en matière numériques ou en matière de procédures dérogatoires qui sera abordé ultérieurement[77].
2° Les données collectées par perquisition ou saisie

[77] V. *infra* n°40 s.

28. Dispositions générales – Dans le but de recueillir des éléments de preuve, l'autorité judiciaire en charge de l'enquête peut faire procéder à des perquisitions et saisies au domicile[78] d'un individu. Lors d'une enquête préliminaire, la perquisition ne peut, par principe, se faire sans le consentement de l'intéressé[79]. Toutefois, si l'enquête porte sur un délit puni d'une peine d'emprisonnement supérieure ou égale à trois ans, et que les circonstances le justifient, le juge des libertés et de la détention peut autoriser la perquisition même en l'absence de consentement. La Cour de cassation a précisé l'étendue de cette autorisation estimant notamment qu'en l'absence de restrictions par le juge des libertés et de la détention, l'autorisation de procéder à une perquisition pouvait inclure la réquisition d'un serrurier pour ouvrir un coffre-fort[80]. Lors d'une enquête de flagrance, l'officier de police judiciaire peut procéder à une perquisition si elle est nécessaire à prouver les faits. Le consentement de l'intéressé n'est alors pas nécessaire[81]. La loi du 9 juillet 2010[82] est venue étendre le champ d'application de ces dispositions, permettant ainsi à l'officier de police judiciaire d'effectuer une perquisition dans « tout lieu » utile. Elle doit, dans ce cas, être autorisée par le procureur de la République.

Aussi, au cours de la phase d'instruction, le juge d'instruction, ou l'officier de police judiciaire, sur commission rogatoire, peuvent procéder à une perquisition[83]. Le juge d'instruction a donc la possibilité de se rendre lui-même sur les lieux afin de procéder aux constatations. Le législateur est venu encadrer le régime de ces perquisitions en fixant des plages horaires pour leur réalisation[84]. Toutefois, en matière de criminalité organisée[85] les perquisitions hors de ces plages horaires sont possibles[86]. Ces perquisitions peuvent permettre la saisie et mise sous main de justice de tout objet utile à l'enquête[87]. Il peut donc s'agir de documents, données informatiques qui contiennent nécessairement des données à caractère

[78] La jurisprudence constante adopte une interprétation extensive du terme de domicile en matière de perquisitions et saisies. Depuis l'arrêt du 13 octobre 1982, il est admis que « le terme de domicile au sens de l'article 226-4 du code pénal ne désigne pas seulement le lieu où une personne a son principal établissement mais encore le lieu, qu'elle y habite ou non, où elle a le droit de se dire chez elle, quels que soient le titre juridique de son occupation et l'affectation donnée aux locaux ». Cass., crim., 13 octobre 1982, *pourvoi* n° 81-92.708.
S. Rayne, *Perquisitions – saisies – visites domiciliaires*, Répertoire de droit pénal et de procédure pénale, Dalloz, octobre 2008, actualisé en février 2018, 27 - 40.
[79] Art. 76 du code de procédure pénale.
[80] Cass. crim. 6 avril 2013, *pourvoi* n°12-86.275.
[81] Art. 56 du code de procédure pénale.
[82] Loi n°2010-768 du 9 juillet 2010 visant à faciliter la saisie et la confiscation en matière pénale.
[83] Art. 92 du code de procédure pénale.
[84] Art. 59 du code de procédure pénale « Sauf réclamation faite de l'intérieur de la maison ou exceptions prévues par la loi, les perquisitions et les visites domiciliaires ne peuvent être commencées avant 6 heures et après 21 heures ».
[85] Art. 706-73 du code de procédure pénale.
[86] Art. 706-92 du code de procédure pénale.
[87] v. art. 54 et 99 du code de procédure pénale.

personnel. Ces données se retrouvent par ce biais intégrées au dossier de procédure comme données à vocation probatoire.

3° Les données interceptées

29. Le développement de procédés d'interception de données – Dans le cadre d'une procédure, les preuves peuvent être collectées par le recours à des procédés d'interception de données. Ces dispositifs encadrés par la loi ont vu leur nombre croitre depuis les années 2000. Cette évolution a été rendue possible à la fois par les développements technologiques permettant l'accès à de nouvelles données et aussi par l'adoption de nouvelles dispositions législatives en la matière. Ces procédés ont soulevé des interrogations du fait de leur caractère intrusif, en termes de respect de la vie privée notamment. Très encadrés par le législateur, ces procédés relèvent pour beaucoup de régimes dérogatoires au droit commun[88]. Les articles 100 et suivants du code de procédure pénale, prévoient la possibilité de recourir au procédé d'écoutes téléphoniques lors de la phase d'instruction en matière criminelle et correctionnelle si la peine encourue est supérieure ou égale à trois ans d'emprisonnement[89]. Le procédé est alors soumis au contrôle du juge d'instruction. Les données recueillies par le biais d'écoutes judiciaires lors d'enquêtes ou d'instruction font l'objet d'un traitement automatisé. Depuis le décret du 9 octobre 2014[90], les données sont stockées sur la « plateforme nationale des interceptions judiciaires » qui permet une consultation par les magistrats ou officiers de police judicaire[91]. Dans le but de faciliter la constatation des infractions et la collecte de preuves, la plateforme stocke et met à disposition des magistrats les données collectées par le biais d'interceptions judiciaires et celles collectées sur réquisitions judiciaires visant les données de connexion. La Commission nationale de l'informatique et des libertés a rendu un avis s'agissant du projet de décret. Dans celui-ci elle fait référence à « un traitement de données à caractère personnel […] d'une grande

[88] V. *infra* n°40 s.
[89] La loi n°2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice a augmenté de deux à trois ans les peines minimum visées.
[90] Décret n°2014-1162 du 9 octobre 2014 portant création d'un traitement automatisé de données à caractère personnel dénommé « Plate-forme nationale des interceptions judiciaires ».
[91] V. s*upra* n°152.

sensibilité » alertant de fait sur les risques d'un tel traitement au vu de la nature des données visées[92].

30. La géolocalisation, procédé d'interception de données de droit commun – Le recours au dispositif de géolocalisation a été institué par la loi du 28 mars 2014[93]. Ce procédé repose sur la mise en œuvre de *« tout moyen technique destiné à la localisation en temps réel, sur l'ensemble du territoire national, d'une personne, à l'insu de celle-ci, d'un véhicule ou de tout autre objet, sans le consentement de son propriétaire ou de son possesseur »*[94]. La géolocalisation permet de recueillir en temps réel des données relatives à la situation géographique d'un objet ou véhicule et à ses déplacements. Grâce à ces données, il est possible directement ou indirectement de rattacher la situation géographique de l'objet à un individu ce qui en fait un moyen de collecte de données à caractère personnel au sens de la loi informatique et libertés et du règlement général sur la protection des données. Ces données peuvent ensuite être analysées et utilisées comme preuves dans une procédure. Les articles 230-32 et suivants du code de procédure pénale fixent les modalités de mise en œuvre d'un tel dispositif. Ainsi, il peut être recouru à la géolocalisation lors d'une enquête ou d'une instruction portant sur des crimes ou délits punis d'au moins trois ans d'emprisonnement, portant sur la recherche de cause de la mort, ou la recherche d'une personne en fuite. La loi a été soumise au contrôle *a priori* du Conseil constitutionnel qui dans sa décision du 25 mars 2014[95] a prononcé la validité de cette dernière s'agissant de la mise en œuvre de la mesure. Toutefois, le Conseil constitutionnel a prononcé la censure partielle de certaines dispositions relatives au dossier de procédure[96]. La loi initiale prévoyait que les données recueillies par géolocalisation puissent faire l'objet d'un dossier distinct afin notamment de protéger les personnes ayant permis l'installation du dispositif. Le Conseil constitutionnel a considéré qu'afin de respecter les droits de la défense, la personne mise en cause devait nécessairement avoir connaissance de toutes les données afin de pouvoir, le cas échéant, faire jouer son droit

[92] Délibération CNIL n°2014-009 du 16 janvier 2014 portant avis sur un projet de décret autorisant la mise en œuvre d'un traitement automatisé de données à caractère personnel dénommé « Plateforme nationale des interceptions judiciaires ».

[93] Loi n°2014-32 du 28 mars 2014 relative à la géolocalisation. Rappelons que la Cour européenne des droits de l'homme s'est prononcée dans l'arrêt Uzun c/ Allemagne du 2 septembre 2010 sur la légalité d'un tel dispositif. Au vu de son caractère très intrusif, elle a considéré qu'il devait nécessairement être encadré par la loi afin d'être en conformité avec l'article 8.
H. Matsopoulou, L'illégalité des surveillances par « géolocalisation » autorisées par le ministère public, *Dalloz*, 2014, p. 115.

[94] Art. 230-32 du code de procédure pénale.

[95] Décision 2014-693 DC du 25 mars 2014.

[96] C. Fleuriot, Géolocalisation : censure partielle pour violation des droits de la défense, *Dalloz actualité*, 27 mars 2014.

de contestation sur les données en question. Ainsi, les articles 230-38 et 230-39 du code de procédure pénale disposent que les données recueillies qui sont utiles à la manifestation de la vérité font l'objet d'un procès-verbal versé au dossier. Toutefois une dérogation est possible en matière de criminalité ou délinquance organisées, les données peuvent alors ne pas apparaitre dans le dossier, mais dans un dossier distinct, sur autorisation du juge des libertés et de la détention[97].

4° Les données collectées par le recours aux expertises

31. Expertises et données à caractère personnel – Que ce soit en matière pénale ou civile le recours aux expertises permet d'apporter une analyse technique sur un dossier. En ce sens, peuvent être demandées des expertises de toute nature. Certaines d'entre elles visent à apporter des éléments relatifs aux individus d'ordre biologique ou médical notamment, et contiennent en cela des données personnelles qui peuvent de plus constituer parfois des données dites « sensibles » au sens du règlement général sur la protection des données. Il s'agit donc de s'interroger sur la procédure permettant le recours aux expertises tant en matière pénale que civile en ce qu'elle engendre la collecte de données à caractère personnel. Les questions plus spécifiques attachées à l'éventuel caractère sensible ou secret de certaines données seront abordées ultérieurement[98].

32. Les expertises en matière pénale – Lorsque les nécessités de l'enquête l'exigent, le juge d'instruction peut ordonner la réalisation d'une expertise. Cette dernière peut être demandée par le ministère public ou une partie, la décision revenant toujours au juge d'instruction[99]. L'expertise peut reposer sur des objets très variés et toucher à des domaines tels que la médecine, la toxicologie, la biologie... Elle permet d'obtenir des informations et une compréhension de la situation que les magistrats seuls n'auraient pas pu avoir. Ces derniers restent toutefois libres dans l'appréciation des rapports qui leurs sont remis[100]. Aussi, les rapports d'expertise versés au dossier sont, comme toute pièce, soumis au principe du

[97] Art. 230-40 du code de procédure pénale. *« Lorsque, dans une instruction concernant l'un des crimes ou délits entrant dans le champ d'application des articles 706-73 et 706-73-1, la connaissance de ces informations est susceptible de mettre gravement en danger la vie ou l'intégrité physique d'une personne, des membres de sa famille ou de ses proches et qu'elle n'est ni utile à la manifestation de la vérité, ni indispensable à l'exercice des droits de la défense, le juge des libertés et de la détention, saisi à tout moment par requête motivée du juge d'instruction, peut, par décision motivée, autoriser que n'apparaissent pas dans le dossier de la procédure ».*
[98] V. *infra* n°102 s.
[99] Art. 156 du code de procédure pénale.
[100] Art. 158 du code de procédure pénale.

contradictoire et peuvent être contestés par les parties. L'expert est désigné par le juge d'instruction sur une liste dressée par la Cour d'appel. Très souvent, l'expertise permet d'apporter un regard plus technique sur une situation et révèle des données qui peuvent avoir une vocation probatoire. La question de la place de l'expertise dans le procès a fait l'objet de nombreux écrits et plus précisément la question de son rôle parfois déterminant dans l'intime conviction du juge[101].

5° Les procédés de collecte de données à vocation probatoire à l'étranger

33. La collecte de données probatoires hors du territoire – La question se pose également du recueil de preuves à l'étranger et plus exactement des procédés permettant l'obtention de données auprès d'organismes se situant hors du territoire national[102]. De manière générale, ces questions relèvent de conventions internationales et dépendent de la nature du contentieux[103].

a° La collecte de preuves civiles et commerciales à l'étranger

34. Simplification de la collecte probatoire à l'étranger – La Convention de la Haye du 18 mars 1970[104] est venue préciser le formalisme des commissions rogatoires permettant l'obtention de données probatoires à l'étranger. Elle permet également, dans le cadre d'une procédure ouverte, à un agent diplomatique de réaliser des actes d'instruction en rapport avec cette procédure. Le règlement européen du 28 mai 2001[105] est venu simplifier la procédure par la création de formulaires type permettant la transmission des demandes de preuves. Ces mécanismes relèvent de la compétence dans chaque Etat d'autorités spécifiques (il s'agit en France du bureau de l'entraide civile et commerciale au ministère de la justice). Le règlement offre la possibilité pour un juge de réaliser directement des actes d'instruction à l'étranger[106].

[101] H. Lavedrine, *L'expertise judiciaire*, Y. Mayaud (dir.), Master de droit pénal et sciences pénales, Université Panthéon-Assas Paris II, 2014.
[102] La question du partage de données sera traitée dans le titre 2 relatif au partage de données fichées.
[103] E. Vergès, G. Vial, O. Leclerc, *Le droit de la preuve*, PUF, 2015, *op. cit*.
[104] Convention du 18 mars 1970 sur l'obtention des preuves à l'étranger en matière civile ou commerciale.
[105] Règlement CE n°1206/2001 du 28 mai 2001 relatif à la coopération entre les juridictions des états membres dans le domaine de l'obtention des preuves en matière civile et commerciale.
[106] P. Dubarry, « L'obtention des preuves en France et à l'étranger », *Semaine juridique*, édition générale, n°28, 14 juillet 2014, p. 1418.

b° La collecte de preuves pénales à l'étranger

35. Entraide pénale judiciaire – L'obtention de preuves à l'étranger relève du système d'entraide pénale judiciaire régit par le Conseil de l'Europe et l'Union européenne s'agissant des Etats membres. Ainsi, la convention d'entraide judiciaire du 20 avril 1959[107] a posé les bases d'une coopération internationale, permettant à un Etat de recueillir des preuves auprès d'un autre Etat signataire par l'audition de témoins, d'experts ou de prévenus ou par l'accès aux données du casier judiciaire d'un ressortissant de cet Etat signataire. Plusieurs protocoles additionnels sont venus compléter la convention afin notamment de faciliter la procédure et d'imposer une exigence de célérité dans le traitement des demandes[108].
Au niveau de l'Union européenne, l'obtention de preuves à l'étranger repose sur les accords de Schengen et plus précisément la convention d'application du 14 juin 1985[109] ainsi que sur la convention du 29 mai 2000 relative à l'entraide judiciaire qui est venue simplifier la procédure. Ainsi, cette demande de preuves peut reposer sur la transmission de commissions rogatoires, de demandes d'instruction ou de mandat européen d'obtention de preuves.

36. Les commissions rogatoires internationales – Les commissions rogatoires internationales permettent, comme en matière civile, à un magistrat français de faire exécuter en son nom une mesure d'instruction permettant le recueil ou la recherche de preuves. L'article 694 du code de procédure pénale encadre le recours aux commissions rogatoires qui seraient délivrées en dehors de toute convention. Il précise alors que toute demande de mesures d'instruction faite par la France à un autre Etat non membre de l'Union européenne se fait par le biais du ministère de la justice. Les articles 695 et suivants du code de procédure pénale régissent les demandes adressées à un autre Etat membre. Les commissions rogatoires internationales ont pu être qualifiées « d'actes mixtes »[110]. En effet elles représentent un pilier de la coopération internationale mais le principe de souveraineté nationale impose que les actes soient soumis à la loi du pays dans lequel ils sont réalisés.

[107] Convention européenne d'entraide judiciaire en matière pénale, 20 avril 1959.
[108] Protocole adopté le 19 septembre 2001.
[109] Convention d'application de l'accord de Schengen du 14 juin 1985 entre les gouvernements des Etats de l'Union économique Benelux, de la République fédérale d'Allemagne et de la République française, relatif à la suppression graduelle des contrôles aux frontières communes.
[110] Voir notamment le rapport de la Cour de cassation de 2017 relatif au « juge et à la mondialisation ».

37. Le mandat européen d'obtention de preuves – En application des principes de reconnaissance mutuelle[111] a été créé le mandat européen d'obtention de preuves qui remplace, entre les Etats membres, le recours à la commission rogatoire internationale. Ainsi, le mandat d'obtention de preuves a été créé par la décision-cadre du Conseil du 18 décembre 2008[112]. Ce mandat permet d'obtenir d'un autre Etat membre la transmission d'objets, de documents ou de données[113]. Si l'Etat destinataire juge ces éléments pertinents, ils sont transmis sans délai au pays demandeur. Toutefois, ce mandat ne peut viser l'obtention d'interrogatoires, le recueil de données biologiques ou biométriques, l'interception de communications, ou l'obtention d'extrait de casier judiciaire[114]. Ce mandat vise la production de données déjà en la possession des autorités et qui sont précisées dans la demande. Néanmoins, l'Etat d'exécution peut, s'il le juge utile, transmettre des documents ou objets qui n'ont pas été demandés. Les mandats permettent donc le recueil de données à caractère personnel à vocation probatoire à l'étranger. S'agissant de ces données la décision-cadre précise qu'elles ne peuvent être utilisées que dans le cadre de la procédure dans laquelle le mandat a été émis, de procédures liées ou afin de « prévenir un danger immédiat et sérieux pour la sécurité publique »[115].

38. Le gel de biens ou de preuves – Afin de préserver des données utiles à une procédure en cours, une demande de gel de biens ou d'éléments de preuve[116] peut être déposée auprès d'autorités étrangères. L'autorité judiciaire demanderesse peut alors imposer à l'autorité étrangère d'exécution de respecter certaines formalités sous réserve de ne pas contrevenir aux principes fondamentaux de l'Etat. La procédure vise à empêcher l'altération éventuelle des preuves ou toute modification ou destruction des données, conférant à l'autorité demanderesse un certain pouvoir sur celles-ci en empêchant la réalisation de toute action.

39. Les demandes d'instruction et d'enquête présentées à une autorité judiciaire étrangère – La directive européenne du 3 avril 2014[117] permet de mettre en œuvre des mesures qui n'étaient pas possible avec le mandat d'obtention de preuves en ouvrant une

[111] Le traité sur le fonctionnement de l'Union européenne prévoit aux articles 82 et 83 des règles visant notamment l'admissibilité des preuves transfrontalières au nom du principe de reconnaissance mutuelle.
[112] Décision-cadre du Conseil 2008/978/JAI relative au mandat européen d'obtention de preuves.
[113] Art. 1er de la décision-cadre du Conseil 2008/978/JAI relative au mandat européen d'obtention de preuves.
[114] Art. 4 de la décision-cadre du Conseil 2008/978/JAI relative au mandat européen d'obtention de preuves.
[115] Art. 10 de la décision-cadre du Conseil 2008/978/JAI relative au mandat européen d'obtention de preuves.
[116] Décision-cadre 2003/577/JAI du Conseil du 22 juillet 2003.
[117] Directive du Parlement européen et du Conseil 2014/41/UE du 3 avril 2014 concernant la décision d'enquête européenne en matière pénale.

enquête européenne. Cette dernière permet donc d'effectuer des auditions, d'intercepter des communications…et toute mesure d'enquête qui serait nécessaire et proportionnée, en vue d'obtenir des preuves.

La demande peut émaner des autorités mais aussi d'un suspect ou une personne poursuivie en vertu des droits de la défense. La procédure permet de mettre en œuvre toute mesure d'enquête exception faite de la création d'une équipe commune d'enquête. Cette procédure doit être mise en œuvre dans les 90 jours qui suivent la demande. Il faut préciser, de plus, que l'Etat destinataire de la demande d'enquête européenne ne peut s'y opposer qu'à la condition que celle-ci porte atteinte à ses intérêts ou aux principes fondamentaux consacrés dans cet Etat.

En pratique, cette procédure permet le transfèrement temporaire de personnes détenues afin de recueillir leur témoignage, l'accès au compte bancaire de suspects, la mise en place de dispositifs d'interception de communications et des mesures de conservation de preuves. De fait, la mesure d'enquête européenne constitue un procédé permettant un important recueil de preuves donnant accès notamment à des données à caractère personnel sensibles et protégées détenues par un autre Etat membre.

A côté du régime de droit commun, le législateur a défini des régimes dérogatoires qui permettent la collecte de données probatoires par le recours à des dispositifs particuliers.

B. La collecte de données probatoires relevant de procédés dérogatoires

40. L'extension des régimes dérogatoires – La collecte de données à vocation probatoire peut relever de dispositions dites dérogatoires au droit commun qui par principe offrent des moyens d'accès et de recueil plus importants. La fin du vingtième siècle a été marquée par l'adoption de différentes lois étendant le champ d'application des régimes dérogatoires sur le fondement d'une lutte plus efficace contre certaines formes de criminalité. Cette extension des régimes dérogatoires facilite l'accès à grand nombre de données par l'attribution de moyens spécifiques et soulève donc des interrogations en termes de traitement de données à caractère personnel.

41. Le cadre des régimes dérogatoires – La loi du 9 mars 2004 dite Perben II est venue insérer dans le livre IV du code de procédure pénale des dispositions relatives aux « procédures particulières » et ce dernier a connu une forte évolution par la suite. La doctrine a fait référence à plusieurs types d'extension de ces régimes dérogatoires. Il peut s'agir

d'appliquer à des nouvelles infractions un régime dérogatoire existant, de pérenniser un régime dérogatoire initialement à vocation temporaire ou encore de créer un régime dérogatoire commun à différentes infractions[118]. Face au développement de nouvelles formes de criminalités, les régimes dérogatoires procurant des prérogatives exceptionnelles en termes d'investigations et de recueil de preuves se sont développés, permettant, par le recours à des procédés plus intrusifs, la collecte de données à vocation probatoire. La lutte contre les infractions à caractère terroriste ou contre la criminalité organisée ont conduit le législateur à adopter des lois instaurant ces régimes dérogatoires au droit commun[119].

42. Un développement nécessaire de moyens face aux nouvelles formes de criminalité – Le renforcement de la lutte contre le terrorisme a également entrainé le développement de nouveaux procédés de lutte numériques permettant une meilleure répression de ces infractions[120]. C'est le cas par exemple de l'enquête sous pseudonyme. La loi du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme permet en matière de criminalité organisée et de terrorisme de recourir au dispositif d'enquête sous pseudonyme sur internet[121]. Force est de constater que le développement d'internet a entrainé celui de nouvelles formes de criminalité qui a nécessité la création de nouveaux moyens d'action. En ce sens, internet a permis le développement de nouvelles formes d'enquête et de collecte de preuves. Ainsi, le régime des interceptions de données relève largement d'un régime dérogatoire (1°), la collecte de données à vocation probatoire se trouve facilité par le recours aux régimes dérogatoires (2°).

---

[118] E. Rubi-Cavagna, L'extension des procédures dérogatoires, *RSC*, 2008, p. 23. S'agissant de l'extension du régime dérogatoire par la création d'un régime commun à plusieurs infractions, l'auteure cite la création du régime applicable en matière de criminalité organisée créé par la loi du 9 mars 2004 dite Perben II et dont les infractions sont fixées aux articles 706-73 et 706-74 du code de procédure pénale.

[119] La loi n°96-647 du 22 juillet 1996 tendant à renforcer la répression du terrorisme et des atteintes aux personnes dépositaires de l'autorité publique ou chargées d'une mission de service public et comportant des dispositions relatives à la police judiciaire, est venue modifier l'article 706-16 du code de procédure pénale visant directement les infractions terroristes. A noter qu'avant cela, la loi du 9 septembre 1986 insère dans le code de procédure pénale les premières dispositions relatives aux troubles à l'ordre public par l'intimidation ou la terreur. Elle constitue les prémices de l'arsenal de lutte contre le terrorisme. Ensuite, la loi n°2004-204 du 9 mars 2004 portant adaptation de la justice aux évolutions de la criminalité, marque une des évolutions majeures en insérant dans le code de procédure pénale des dispositions relatives à la criminalité organisée. La loi n°2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme**,** a instauré dans le code pénal des dispositions relatives au délit d'entreprise terroriste individuelle**.** La loi n°2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne a permis le recours aux perquisitions, hors plage horaire légale, dans des locaux autres que le domicile de la personne concernée. Elle a de fait étendu une dérogation qui existait en matière de perquisition domiciliaire.

[120] M. Quéméner, Les nouvelles dispositions de lutte contre la cybercriminalité issues de la loi du 13 novembre 2014 renforçant la lutte contre le terrorisme, *AJ Pénal*, 2015, p. 32.

[121] Art. 706-73 du code de procédure pénale. Ce dispositif est également applicable en matière d'atteintes aux systèmes de traitements automatisés de données (Art. 706-72).

1° Le régime des interceptions de données relevant largement d'un régime dérogatoire

43. Les interceptions de correspondances émises par voie de télécommunication – Initialement réservées au cadre de l'instruction, les écoutes judiciaires sont désormais possibles en phase d'enquête menées dans le cadre d'un régime dérogatoire, depuis la loi du 9 mars 2004[122] en matière de criminalité organisée. L'article 706-95 du code de procédure pénale prévoit la possibilité, sur autorisation du juge des libertés et de la détention saisi sur requête du procureur de la République, d'intercepter des correspondances numériques. Ce procédé est possible en matière notamment de criminalité organisée ou de crimes et délits graves[123] et reste soumis au contrôle du juge qui l'a autorisé.

44. La saisie de correspondances numériques – Les autorités peuvent sur autorisation du juge des libertés et de la détention, saisi par le procureur de la République, saisir à distance des données numériques, les enregistrer et les stocker[124]. Ce procédé peut être ordonné par le juge d'instruction dans le cadre d'une information judiciaire[125]. Contrairement aux écoutes mises en œuvre par application des articles 100 et suivants du code de procédure pénale, en matière dérogatoire les dispositions des articles 706-95-1 et suivants permettent l'accès aux correspondances électroniques stockées[126].

45. Le recours aux IMSI-catcher – Initialement mis en œuvre pour les services de renseignement[127], le recours aux IMSI-catcher a été étendu aux autorités judiciaires dans la lutte contre le terrorisme, par la loi du 3 juin 2016[128]. Ce dispositif permet par le biais d'antennes relais de capter des conversations téléphoniques, l'IMSI étant un numéro unique attaché à toute carte SIM. Sans y faire directement référence, la loi a intégré dans le code de procédure pénale de nouvelles dispositions aux articles 706-95-4 et suivants qui permettent le recours à des dispositifs de recueil de *« données techniques de connexion permettant*

[122] C. Guéry, P. Chambon, *Interception de correspondances*, Droit et pratique de l'instruction préparatoire, Dalloz, 2018-2019, chapitre 562.
C. Guéry, *Instruction préparatoire – Actes que le juge d'instruction peut déléguer*, Répertoire de droit pénal et de procédure pénale, Dalloz, juin 2018, Section 3.
[123] Art. 706-73 du code de procédure pénale.
[124] Art. 706-95-1 du code de procédure pénale.
[125] Art. 706-95-2 du code de procédure pénale.
[126] Cass. crim., 8 juillet 2015, *pourvoi* n°14-88.457. Y. Mayaud, *Terrorisme, poursuites et indemnisation*, Répertoire de droit pénal et de procédure pénale, Dalloz, janvier 2018, 201.
[127] Loi n°2015-912 du 24 juillet 2015 relative au renseignement.
[128] Loi n°2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale.

l'identification d'un équipement terminal ou du numéro d'abonnement de son utilisateur, ainsi que les données relatives à la localisation d'un équipement terminal utilisé». Ce dispositif peut être utilisé dans le cadre de l'enquête ou de l'instruction.

Dans le cadre de l'enquête, il doit être autorisé par le juge des libertés et de la détention sur requête du procureur de la République pour un mois renouvelable. Il permet dans un premier temps le recueil des données techniques de connexions c'est-à-dire des données personnelles permettant l'identification du titulaire de la ligne et non, par principe, le recueil du détail des correspondances. Ensuite, ce dispositif peut permettre le recueil des correspondances émises ou reçues sur l'appareil visé, toujours sur autorisation du juge des libertés et de la détention saisi par requête du procureur de la République pour une durée initiale de 48 heures.

De la même manière, le juge d'instruction peut, au cours de l'information judiciaire, autoriser le recours à ce dispositif pour une durée de deux mois s'agissant du recueil des données techniques de connexion et de 48 heures s'agissant de recueil des correspondances. Les autorisations prennent la forme d'ordonnances écrites et motivées. Les données recueillies font l'objet de procès-verbaux.

Ce dispositif permet donc le recueil de grand nombre de données à caractère personnel à l'insu de la personne concernée et a soulevé des interrogations en termes de protection du secret des correspondances notamment.

La CNIL s'est prononcée dans une délibération du 5 mars 2015[129] sur le projet de loi renseignement qui a instauré le recours aux IMSI-catcher par les services de renseignement. Elle avait alors relevé le caractère intrusif pour les libertés individuelles d'un tel dispositif et la nécessité que ce dernier fasse l'objet d'une autorisation. La Commission a alors rappelé que des atteintes au droit au respect de la vie privée et à la protection des données à caractère personnel peuvent être justifiées et légitimes au regard du but poursuivi. Néanmoins, ces atteintes doivent être adéquates et proportionnées. Par exemple, la CNIL relève que si la loi encadre les procédés de collecte de données, elle n'apporte aucune rectification s'agissant des fichiers de renseignement existant déjà. S'agissant du recours aux IMSI-catcher, la CNIL insiste sur le fait que ces derniers permettent non pas une collecte des seules « données utiles » mais une collecte massive de données de manière « indifférenciée », ce qui présente un risque important en termes de vie privée et données personnelles et appelle à des garanties importantes.

[129] Délibération CNIL n°2015-078 du 5 mars 2015 portant avis sur un projet de loi relatif au renseignement.

46. La captation de données informatiques – Le recours aux procédés de captation de données informatiques lors de l'enquête découle de la loi du 3 juin 2016. Initialement ce procédé était réservé au juge d'instruction[130] puis a été étendu aux enquêtes en matière de criminalité organisée ou délits visés à l'article 706-73 du code de procédure pénale. Codifiés aux articles 706-102-1 et suivants du code de procédure pénale, ils permettent aux autorités chargées de l'enquête, sur autorisation du juge des libertés et de la détention saisi sur requête du procureur de la République, d'accéder, d'enregistrer, de conserver et transmettre des données informatiques sans le consentement de la personne intéressée. De la même manière, le juge d'instruction peut, après simple avis du procureur de la République, décider de la mise en place d'un tel dispositif s'il estime cela nécessaire. Le dispositif est mis en œuvre sur ordonnance pour une durée initiale d'un mois en matière d'enquête et de quatre mois en matière d'instruction. Les données nécessaires à l'enquête sont retranscrites dans un procès-verbal versé au dossier.

47. La sonorisation et fixation d'images – La loi du 3 juin 2016[131] est venue étendre les possibilités de recours à ce procédé initialement réservé au juge d'instruction. Désormais, l'article 706-96 du code de procédure pénale prévoit la possibilité pour les officiers de police judiciaire, autorisés par le juge des libertés et de la détention sur requête du procureur de la République, de mettre en œuvre des techniques de sonorisation et fixation d'images dans des lieux et véhicules publics ou privés sans le consentement des intéressés. Ce procédé peut toujours être ordonné par le juge d'instruction[132]. La sonorisation et fixation d'images reste néanmoins interdite dans les lieux renfermant des données relevant du secret défense, les cabinets d'avocats, les cabinets médicaux, les locaux de presse, les juridictions, les études de notaires ou d'huissier, le domicile de personnes exerçant des fonctions juridictionnelles.

2° La collecte de données à vocation probatoire facilitée par le recours à des procédés dérogatoires

48. Problématiques attachées à la généralisation des procédés dérogatoires – Le recours aux procédés dérogatoires de recueil de preuve a connu un développement important justifié, en partie, par l'évolution de la criminalité. Le développement des procédures dérogatoires

[130] Loi LOPSI II du 14 mars 2011.
[131] Loi n°2016-731 du 3 juin 2016, renforçant la lutte contre le crime organisé, le terrorise et leur financement et améliorant l'efficacité et les garanties de la procédure pénale.
[132] Art. 706-96-1 du code de procédure pénale.

soulève des questions relatives à la généralisation de ces dernières. Le nombre de procédures dérogatoires augmente, leur champ d'application s'élargit mais au-delà, on assiste parfois à ce que certains désignent comme une « intégration dans le droit commun »[133]. L'extension de telles procédures trouve néanmoins des limites.

49. L'autorisation par le législateur du recours à une procédure dérogatoire pour une infraction relevant du droit commun – En matière de sonorisation et fixation d'images, la loi du 13 novembre 2007[134] est venue étendre le recours à de tels procédés pour les infractions de corruption et trafic d'influence.

Aussi, en matière de perquisition réalisée sans le consentement de l'intéressé, qui était initialement réservée aux procédures liées à une infraction terroriste sur autorisation du juge des libertés et de la détention, la procédure a par la suite été étendue aux infractions de criminalité organisée puis à tous les délits punis d'une peine d'au moins trois ans d'emprisonnement[135].

De la même manière, la loi du 23 mars 2019[136] est venue étendre le recours aux procédés de géolocalisation à tout délit puni d'au moins trois ans d'emprisonnement. La Conseil constitutionnel a validé ces dispositions considérant que *« la mise en œuvre de ce procédé n'implique pas d'acte de contrainte sur la personne visée, ni d'atteinte à son intégrité corporelle, de saisie, d'interception de correspondance ou d'enregistrement d'image ou de son»*[137]. Aussi, le contrôle opéré par l'autorité judiciaire et la durée limitée du recours au procédé apporte, selon lui, les garanties nécessaires et *« opère une conciliation équilibrée entre les exigences constitutionnelles »*[138].

On peut également citer le recours au procédé d'enquête sous pseudonyme que la loi du 23 mars 2019 introduit dans le code de procédure pénale à l'article 230-46 pour les crimes et délits commis par voie de communications électroniques. Ces dispositions ont été validées par le Conseil constitutionnel estimant que le droit au procès équitable et le droit au respect de la vie privée sont respectés[139].

[133] E. Rubi-Cavagna, L'extension des procédures dérogatoires, *op.cit.*
[134] Loi n°2007-1598 du 13 novembre 2007 relative à la lutte contre la corruption.
[135] Loi n°2004-204 du 9 mars 2004 portant adaptation de la justice aux évolutions de la criminalité.
[136] Loi n°2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice.
[137] Cons. Const., 2019-778 DC du 21 mars 2019, considérant 148.
[138] Const., 2019-778 DC du 21 mars 2019, considérant 150.
[139] Const., 2019-778 DC du 21 mars 2019, considérant 156.

50. Les limites à l'extension des procédures dérogatoires – On ne peut traiter le sujet de l'extension des procédures dérogatoires sans revenir au moins brièvement sur la réforme pour la justice engagée par la loi du 23 mars 2019[140] et plus précisément sur les dispositions relatives au recueil de données. En ce qui concerne la collecte de données lors des investigations, certaines dispositions ont fait l'objet d'une censure par le Conseil constitutionnel. En effet, le projet de loi prévoyait d'importants changements. Par exemple, il était question d'étendre le champ d'application des écoutes judiciaires à toute infraction punie d'au moins trois ans d'emprisonnement dans le cadre d'une enquête. Bien que cette procédure soit déjà possible lors de la phase d'instruction, cette mesure étendait, de ce fait, la procédure à toute infraction au stade de l'enquête. Aussi, dans sa décision du 21 mars 2019[141], le Conseil constitutionnel a jugé que *« le législateur n'a pas opéré une conciliation équilibrée entre l'objectif de valeur constitutionnelle de recherche des auteurs d'infractions et le droit au respect de la vie privée et le secret des correspondances »*[142]. Le projet de loi prévoyait également l'extension du recours aux techniques spéciales d'enquête (sonorisation, captation d'images, captation de données informatiques). Ces procédés sont réservés aux enquêtes relatives aux délits ou crimes organisés et strictement encadrés. Le projet de loi prévoyait d'étendre le recours à de tels dispositifs à tout crime. Le Conseil constitutionnel rappelle le caractère intrusif de tels dispositifs, qui sont justifiés par la gravité de l'infraction et autorisés par le juge des libertés et de la détention qui peut à tout moment décider de leur interruption. Le Conseil constitutionnel juge alors que le législateur n'a pas apporté les garanties suffisantes quant au contrôle d'un tel dispositif[143] et n'a pas concilié un juste équilibre entre recherche de la vérité et droit au respect de la vie privée[144].

Aux cotés de procédés dérogatoires qui confèrent des prérogatives spéciales en termes de recueil de preuves et d'investigation, on assiste également à un rapprochement des moyens judiciaires et du renseignement. Initialement présentés comme deux systèmes distincts, on constate que la frontière entre les deux n'est pas si perméable, ce qui en soit constitue une dérogation aux dispositions communes.

[140] Loi n°2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice. La loi comprend plusieurs volets relatifs, notamment, à la simplification de la procédure civile, l'allégement de la charge des juridictions administratives, la simplification et renforcement de l'efficacité de la procédure, la réorganisation des juridictions, la justice pénale des mineurs, le sens de la peine.
[141] Cons. Const., 2019-778 DC du 21 mars 2019.
[142] Cons. Const., 2019-778 DC du 21 mars 2019, considérant 147.
[143] Cons. Const., 2019-778 DC du 21 mars 2019, considérant 164.
[144] Cons. Const., 2019-778 DC du 21 mars 2019, considérant 165.

C. La collecte de données judiciaires auprès des services de renseignement : la judiciarisation du renseignement

51. L'ouverture d'une procédure judiciaire sur la base de données collectées par les autorités administratives – Au terme du règlement général sur la protection des données et de la loi informatique et libertés, le traitement de données renvoie à tout procédé visant de manière générale l'accès, l'utilisation, le stockage de celles-ci. Il apparait donc évident que la collecte de données dans le cadre de l'administration de la preuve constitue un traitement de données personnelles. Par extension, il peut être intéressant d'analyser la question de la « judiciarisation » du renseignement en considérant qu'il s'agit du procédé permettant l'ouverture d'une procédure judiciaire sur le fondement de données issues du renseignement. Il ne s'agit donc pas d'une collecte entendue comme un recueil de preuves mais plutôt d'un accès pour les autorités judiciaires à des données à vocation probatoire collectées par le biais de procédures administratives du renseignement et qui ont, par conséquent, vocation à être utilisées comme fondement d'une procédure judiciaire en apportant des éléments et des données nécessaires à l'ouverture d'une telle procédure. Cette question concerne donc bien le sujet du traitement de données à caractère personnel dans une procédure judiciaire en ce que ces données constituent le point de départ d'une procédure judiciaire, devenant ainsi des données judiciaires.

La « judiciarisation » du renseignement soulève la question de la frontière entre administratif et judiciaire, les finalités de chacune tendant à se confondre. Cette question découle nécessairement des lois relatives au renseignement et à la lutte contre le terrorisme et à l'état d'urgence[145]. S'agissant de la question de la donnée intervenant en tant que preuve dans une procédure judiciaire, le constat de l'augmentation des pouvoirs octroyés à la police administrative (1°) amène à s'interroger sur le recours aux données probatoires issues du renseignement (2°)

[145] Notamment la loi n° 2015-1501 du 20 novembre 2015 prorogeant l'application de la loi n° 55-385 du 3 avril 1955 relative à l'état d'urgence et renforçant l'efficacité de ses dispositions ; le décret 2015-1475 du 14 novembre 2015 portant application de la loi du 3 avril 1955 ; loi n° 2016-162 du 19 février 2016 prorogeant l'application de la loi n° 55-385 du 3 avril 1955 ; loi n° 2016-629 du 20 mai 2016 prorogeant l'application de la loi n° 55-385 du 3 avril 1955 ; loi n° 2016-987 du 21 juillet 2016 prorogeant l'application de la loi n° 55-385 du 3 avril 1955 relative l'état d'urgence et portant mesures de renforcement de la lutte antiterroriste ; loi n° 2016-1767 du 19 décembre 2016 prorogeant l'application de la loi n° 55-385 du 3 avril 1955 ; loi n° 2017-1154 du 11 juillet 2017 prorogeant l'application de la loi n° 55-385 du 3 avril 1955; loi n° 2015-912 du 24 juillet 2015 relative au renseignement ; loi n° 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme.

1° Le constat préalable de l'augmentation des pouvoirs octroyés à la police administrative

52. Extension des pouvoirs des services administratifs – Ces dernières années ont été marquées par l'extension des pouvoirs accordés aux services administratifs de renseignement leur octroyant parfois des prérogatives similaires à celles des services judiciaires. En ce sens, il faut citer la loi de programmation militaire du 13 décembre 2013[146] et plus particulièrement son article 20. Bien qu'ayant été abrogé par la loi du 24 juillet 2015[147] il est intéressant de noter que cet article prévoyait que lorsqu'étaient en jeu des renseignements intéressant la sécurité nationale, la lutte contre le terrorisme et la délinquance ou la criminalité organisée[148], les services de police administrative pouvaient en temps réel intercepter des données de connexion et récupérer ainsi des « documents » et « informations » des internautes directement auprès des hébergeurs[149]. Ces mesures avaient reçu un accueil très mitigé.

A titre d'exemple, dans une lettre ouverte adressée aux parlementaires, la Fédération internationale des droits de l'Homme et la Ligue des droits de l'Homme avaient appelé ces derniers à saisir le Conseil constitutionnel[150]. Elles estimaient qu'au vu de l'étendue des données visées par ces mesures et le manque de contrôle exercé sur ces collectes en termes de nécessité et de proportionnalité, ces dispositions pouvaient porter une atteinte excessive aux droits fondamentaux et notamment au droit au respect de la vie privée[151]. La commission nationale de l'informatique et des libertés a déploré de ne pas avoir été consultée pendant la phase d'examen du projet de loi. Elle a dans un premier temps souligné que les termes de « documents et informations » renvoient à une « notion très vague » qui peut en pratique porter une atteinte excessive au droit au respect de la vie privée. Toutefois, dans un second temps, cette dernière a estimé que la référence au nouvel article L. 246-3 du code de la

[146] Loi n° 2013-1168 du 13 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale.
[147] Loi n°2015-912 du 24 juillet 2015 relative au renseignement.
[148] Article L. 241-2 du code de la sécurité intérieure abrogé par la loi du 24 juillet 2015.
[149] Ces documents et informations visent toutes les données permettant d'identifier l'internaute, de localiser la connexion, les communications émises et reçues ainsi que leur durée et leur date.
[150] Suite au vote des sénateurs en deuxième lecture, la FIDH et la LDH ont appelé les parlementaires à saisir le conseil constitutionnel dans une lettre ouverte du 13 décembre 2013.
[151] La Fédération internationale des droits de l'Homme et la Ligue des Droits de l'Homme dénoncent une atteinte au respect de la vie privée, à la liberté d'expression, au droit au recours effectif, au principe d'intelligibilité et d'accessibilité de la loi. Elles estiment également que les dispositions de l'article 20 de la loi vont à l'encontre de l'article 34 de la Constitution selon lequel « la loi fixe les règles concernant les droits civiques et les garanties fondamentales accordées aux citoyens pour l'exercice des libertés publiques » ; et de l'article 66 de la Constitution qui dispose que le juge judiciaire et garant des libertés individuelles.

sécurité intérieure[152] qui fixe les modalités de la collecte limite « *toute aspiration massive et directe de données par les services de renseignement* »[153].

53. Augmentation des données collectées – Il convient également de citer la loi du 20 novembre 2015[154] prorogeant l'état d'urgence. Cette dernière avait étendu les pouvoirs en matière de police administrative permettant au ministre de l'intérieur et aux préfets de faire procéder à des perquisitions diurnes et nocturnes, de prononcer des assignations à résidence à l'encontre de toute personne pour laquelle il y a des « raisons sérieuses de penser que son comportement constitue une menace pour la sécurité et l'ordre publics » ou encore de dissoudre des associations qui menacent l'ordre public.

La loi du 24 juillet 2015 relative au renseignement est venue, elle aussi, étendre les prérogatives offertes aux services de renseignement en posant un cadre légal aux pratiques qui pour certaines étaient déjà utilisées[155]. En abrogeant les dispositions antérieures de la loi de programmation militaire, la loi sur le renseignement entend mieux encadrer le traitement des données personnelles afin d'apporter de meilleures garanties en termes de protection de ces données. Cette loi fait suite aux attentas perpétrés à Paris en janvier 2015. Ainsi, elle offre la possibilité pour les services de renseignement lorsqu'il y a une « nécessité d'intérêt public » d'user de moyens de surveillance plus poussés tels que l'interception de sms ou mails, l'utilisation de balises GPS, le piratage d'ordinateurs ou l'installation de logiciels-espions présentés dans un chapitre relatif aux « interceptions de sécurité ». Une des mesures les plus controversées de la loi est le recours aux « IMSI-catchers »[156]. Ce procédé permet d'intercepter sans distinction toutes sortes de données et d'informations issues de conversations téléphoniques. La loi permet également la pose de balises sur les véhicules permettant leur localisation en temps réel. Elle instaure également des procédés d'interception

[152] L'article L. 246-3 du code de la sécurité intérieure prévoit que ce recueil se fait sur sollicitation du réseau et transmis par les opérateurs eux-mêmes. Aussi, l'autorisation de recueil est accordée « sur demande écrite et motivée des ministres de la sécurité intérieure, de la défense, de l'économie.

[153] Délibérations CNIL n°2015-078 du 5 mars 2015 portant avis sur un projet de loi relatif au renseignement. La CNIL insiste set repend les propos du président de la Commission des lois du sénat selon lesquels ces dispositions ne peuvent être utilisées qu'à des fins de géolocalisation en temps réel.

[154] Loi n° 2015-1501 du 2 novembre 2015 prorogeant l'application de la loi n° 55-385 du 3 avril 1955 relative à l'état d'urgence et renforçant l'efficacité de ses dispositions.

[155] O. Desaulnay, R. Ollard, Le renseignement français n'est plus hors-la-loi. Commentaire de la loi n°2015-912 du 24 juillet 2015 relative au renseignement, *Droit pénal*, n°9, sept. 2015, étude 7. R. Ollard, O. Desaulnay, La réforme de la législation anti-terroriste ou le règle de l'exception pérenne, *Droit pénal*, n°1, janvier 2015, étude 1.

[156] Il s'agit d'outils qui permettent, en faisant fonction de fausses antennes relais, d'intercepter les conversations téléphoniques. Ces antennes permettent d'intercepter toutes les données qui entrent ou sortent de l'appareil et également d'accéder au numéro d'autres téléphones qui seraient à proximité de celui-ci. Voir les articles 851-1 et suivants du code de la sécurité intérieure.

de communication pour une durée initiale de 48 heures ou la possibilité de sonoriser des lieux et véhicules ainsi que la captation d'images et de données informatiques. Les données sont conservées pour une durée variant en fonction de leur nature. Ainsi, la loi de 2015 prévoit une conservation de trente jours pour les correspondances, cent-vingt pour les sonorisations, captations d'images et de données informatiques et quatre ans pour les données de connexion. De manière générale, ces procédés permettent de capter des données à caractère personnel relatives à de individus identifiés comme présentant une menace mais également à de tierces personnes en lien plus ou moins étroit avec elles.

54. La Commission nationale de contrôle des techniques de renseignement – La commission nationale de contrôle des techniques de renseignement (CNCTR)[157] exerce en tant qu'autorité administrative indépendante un contrôle sur ces divers procédés et rend un avis sur le recours à ces derniers[158]. Elle dispose aussi d'un *« droit de regard sur les techniques de recueil de renseignement»*[159].

Le 5 mars 2015, la CNIL a rendu un avis[160] sur le projet de loi renseignement[161]. Le cadre législatif ne lui permettant pas d'opérer un contrôle au vu de la loi de 1978, la commission avait dès lors demandé à pouvoir néanmoins exercer un contrôle en coopération avec la commission nationale de contrôle des techniques de renseignement.

Il faut toutefois noter que le Conseil constitutionnel saisi de la question a très largement validé la loi de 2015[162] écartant seulement quelques articles relatifs à la surveillance internationale et à la surveillance des communications hertziennes.

La commission nationale de contrôle des techniques de renseignement a rendu le 13 décembre 2016 son premier rapport annuel[163]. Il ressort, par exemple, qu'entre octobre 2015 et octobre 2016 la commission a rendu 48208 avis relatifs à l'accès aux données de connexion, 8538 avis relatifs aux interceptions de sécurité et 2127 avis relatifs à la géolocalisation en temps réel. Aussi, 20282 personnes auraient été visées par une technique de renseignement sur cette même période. Le contrôle a postériori semble néanmoins plus difficile à mettre en œuvre les

[157] Commission créée le 3 octobre 2015 en remplacement de Commission nationale de contrôle des interceptions de sécurité.
[158] Voir, délibération de la CNCTR n° 2/2016 du 10 novembre 2016, JORF 30 décembre 2016.
[159] Voir à ce sujet, R. Parizot, « Surveiller et prévenir…à quel prix ? Loi n° 2015-812 du 24 juillet 2015 relative au renseignement », *JCP G*, n° 41, 5 oct. 2015, doctr., 1077.
[160] Délibération CNIL n° 2015-078 du 5 mars 2015 portant avis sur un projet de loi relatif au renseignement.
[161] Avis rendu public à la demande du Président de la commission des lois de l'Assemblée Nationale, M. Urvoas.
[162] Cons. const. , décision n° 2015-713 DC du 23 juillet 2015.
[163] Voir, L. Chataignier, A. Geraud, T. Gauthier, « L'Etat de droit à l'épreuve du renseignement : Bilan du premier rapport d'activité de la CNCTR », *La revue des droits de l'Homme,* février 2017.

données étant dans certains cas décentralisées[164]. La commission n'a toutefois jamais été saisie directement par un service de renseignement lui-même. Le défenseur des droits[165] avait également exprimé quelques réserves liées notamment au fait que selon lui « l'intérêt public » visé par la loi n'est pas défini de manière suffisamment « précise et restrictive ». Aussi, il demandait dès lors que soit précisé le lien entre renseignement et procédure judiciaire abordant ainsi la question de la judiciarisation du renseignement[166].

2° Le recours aux données probatoires issues du renseignement

55. Notion de judiciarisation – La judiciarisation du renseignement vise le procédé qui permet l'ouverture d'une procédure judiciaire sur le fondement de données collectées dans le cadre du renseignement ou suite à la mise en œuvre d'une mesure de police administrative. La notion même de « judiciarisation » soulève de nombreuses controverses et elle ne saurait en réalité se limiter aux seules questions relatives à l'administration de la preuve. Ce sont toutefois ces questions qui intéressent le sujet du recueil de preuves. Il s'agit donc ici d'appréhender la question de la judiciarisation du renseignement comme un procédé ayant pour conséquence pour les autorités judiciaires de collecter des données par le biais des services de renseignements, ces données ouvrant alors une procédure judiciaire et entrainant le traitement de ces données. En ce sens, il peut sembler opportun de parler de « traitement judiciaire du renseignement »[167]. Une telle approche des deux procédures soulève évidemment la question du respect de la légalité de la procédure pénale d'un côté et de la protection des donnés du renseignement de l'autre et notamment du secret défense[168].

56. Quelques exemples de « judiciarisation » du renseignement – Concernant les mesures administratives, il s'agit par exemple des mesures d'interdiction de sortie du territoire prévues à l'article L. 224-1 du code de la sécurité intérieure et prononcées sur décisions du ministre de

[164] Par exemple dans le cas des IMSI-catcher. A noter que sinon les données recueillies sont centralisées par le Groupement interministériel de contrôle et que la CNCTR dispose d'un accès direct à ces informations.
La commission a relevé que si l'article L. 871-2 du code de la sécurité intérieure permet au Premier ministre de demander aux fournisseurs de services de communication toutes les informations utiles à la mise en œuvre des interceptions, l'article L. 852-1 du même code prévoit l'avis de la CNCTR. Le Premier ministre a par la suite fait savoir qu'il s'alignerait sur les dispositions de l'article L. 852-1.
[165] Communiqué du 13 avril 2015.
[166] Voir à ce sujet, R. Noguellou, « Projet de loi relatif au renseignement : le Défenseur des droits exprime ses réserves, *JCP A*, n° 6, juin 2015.
[167] Pour reprendre le terme utilisé par P. Fourre, *La judiciarisation du renseignement*, Colloque sur « Le renseignement de sécurité et de défense », Forum de recherche de l'AFDSP, 25 juin 2020.
[168] *Ibid.*

l'intérieur. Le code pénal prévoit une sanction au non respect de ces dispositions[169]. Un autre exemple de ce phénomène peut être constaté par l'adoption des dispositions du code de la sécurité intérieure à l'article L.225-7[170]. Ainsi, lorsqu'une personne a quitté le territoire et qu'il existe des « raisons sérieuses » de croire que ce déplacement avait un but terroriste, cette dernière peut faire l'objet d'un contrôle administratif à son retour en France. Le procureur de Paris ainsi que le procureur territorialement compétent sont informés par l'autorité administrative qui peut imposer certaines obligations à la personne concernée. Il peut s'agir par exemple, de l'obligation de résider dans un « périmètre géographique déterminé » ou de se présenter périodiquement aux autorités[171]. L'article L. 225-7 du code de la sécurité intérieure prévoit que le non respect de ces obligations est puni de trois ans d'emprisonnement et de 45000 euros d'amende. Ces dispositions renvoient de toute évidence à une sanction pénale.[172]

57. La valeur probatoire du « renseignement judiciaire » – La judiciarisation du renseignement conduit à s'interroger sur la potentielle valeur probatoire dans une procédure judiciaire de données issues du renseignement. Au-delà des interrogations liées aux garanties nécessaires à la collecte par le judiciaire de données du renseignement ou des finalités de cette même donnée qu'elle soit traitée par l'administration ou par le judiciaire, se pose la question de la possible collecte de preuves auprès des services de renseignement. Dans cette optique on peut cesser d'opposer le judiciaire et l'administratif et concéder que finalement la frontière entre les deux s'amenuise notamment du fait des nouvelles formes de criminalité. Le terrorisme constitue un parfait exemple qui pousse à s'interroger sur l'existence de cette frontière en termes d'administration de la preuve. Il a en ce sens été soulevé le fait qu'une donnée relative à une activité terroriste peut constituer à la fois une donnée de renseignement en ce qu'elle permet la prévention de tels actes par les services de renseignement et elle peut tout autant constituer une potentielle preuve de ces agissements dans une procédure judiciaire[173].

---

[169] Il s'agit de l'infraction constituée par la tentative ou le fait de quitter le territoire français en violation d'une interdiction de sortie du territoire.
Voir à ce sujet, Y. Mayaud « L'état d'urgence récupéré par le droit commun ? Ou de l'état d'urgence à l'état de confusion ! », *JCP G*, 2016, doctr. 344.

[170] Dispositions insérées par la loi n°2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement et améliorant l'efficacité et les garanties de la procédure pénale.

[171] Voir les dispositions des articles L. 225-1 et suivants du code de la sécurité intérieures.

[172] Voir à ce sujet les recherches de JB. Thierry, Maître de conférences en droit privé, *Sinilege.hypothèses.org.*

[173] B. Hurel, *Les difficultés relatives à la judiciarisation*, Colloque sur « Le renseignement au service de l'enquête », Institut national des hautes études de la sécurité et de la justice, 21 mai 2019.

58. Les données du renseignement alimentant les procédures judiciaires – En matière de lutte contre le terrorisme, le mécanisme de judiciarisation constitue une des « trois sources » d'ouverture d'une enquête judiciaire[174]. Sur la base d'éléments et de données transmises aux autorités, une enquête judiciaire peut être ouverte et permet par la suite le recours aux procédures dérogatoires permises en la matière. La judiciarisation peut donc s'analyser comme une coopération nécessaire et efficace à la condition de trouver le juste équilibre ménageant les deux procédures.

Le Conseil constitutionnel semble pourtant attaché à la distinction entre administratif et judiciaire, rappelant dans une décision du 23 juillet 2015, que « le recueil de renseignement au moyen des techniques définies au titre V du livre VIII du code de la sécurité intérieure par les services spécialisés de renseignement pour l'exercice de leurs missions respectives relève de la seule police administrative ; qu'il ne peut donc avoir d'autre but que de préserver l'ordre public et de prévenir les infractions ; qu'il ne peut être mis en œuvre pour constater des infractions à la loi pénale, en rassembler les preuves ou en rechercher les auteurs »[175].

Toutefois l'article L811-2 du code de sécurité intérieure précise que les dispositions du même code qui encadrent le recueil de renseignements ne peuvent porter préjudice aux dispositions de l'article 40 du code de procédure pénale[176].

Le principe de légalité de la preuve tend donc à encadrer certains modes de collecte notamment les procédés coercitifs, il constitue également un obstacle dans la liberté reconnue à chacun dans cette collecte en ce qu'il trouve une limite dans le respect des droits et libertés.

§2. Le respect de la légalité matérielle

59. Notion de légalité « matérielle » – Le principe de légalité de la preuve renvoie également aux obstacles qui peuvent se présenter dans la collecte de données probatoires attachés notamment au droit au respect de la vie privée ou au respect de la dignité humaine. Il s'agit ici de la légalité dite « matérielle » qui par principe tend à s'appliquer à tous y compris aux

[174] S. Goy-Chavent, *Menace terroriste, pour une République juste mais plus ferme*, Rapport de la Commission d'enquête déposé le 4 juillet 2018.

[175] Cons. Const., 23 juillet 2015, 2015-713DC, cons. 9.

[176] Art. 40 du code de procédure pénale « Toute autorité constituée, tout officier public ou fonctionnaire qui, dans l'exercice de ses fonctions, acquiert la connaissance d'un crime ou d'un délit est tenu d'en donner avis sans délai au procureur de la République et de transmettre à ce magistrat tous les renseignements, procès-verbaux et actes qui y sont relatifs ». Voir, F. Fourment, La loi « Renseignement », le renseignement incident de commission d'une infraction et l'autorité judiciaire, *in*, « Le renseignement dans un dossier pénal », *Gazette du palais*, 26 janvier 2016.

particuliers bien que la pratique conduit à l'appliquer notamment aux autorités dans l'usage de procédés coercitifs en matière pénale. La collecte de données à vocation probatoire peut se trouver confrontée au principe du respect de la vie privée (A.) et au respect de la dignité humaine (B.).

A. La collecte de données personnelles à vocation probatoire confrontée au principe du respect de la vie privée

60. Portée de la légalité comme obstacle à la preuve – La question de la portée de la légalité de la preuve se pose notamment s'agissant de la collecte et de la production de données issues de correspondances ou de captations de données faites à l'insu des individus concernés.
Il faut s'interroger sur l'application du principe de légalité au regard notamment de la consécration du droit à la preuve.
Il faut s'interroger sur l'application du principe de légalité en matière de production de correspondances (1°), en matière de captation d'images (2°) et aborder séparément la question de la collecte de preuves dans l'entreprise (3°).

1° L'application du principe de légalité en matière de production de correspondances

61. Vie privée et droit à la preuve – L'article 9 du code civil pose le principe du respect de la vie privée duquel découle notamment le droit à la protection du secret des correspondances[177]. Dans un arrêt du 5 avril 2012[178], la première chambre civile de la cour de cassation a du se prononcer sur la licéité d'une lettre produite en justice sans autorisation des auteurs. Par cet arrêt, la cour de cassation va reconnaitre l'existence d'un droit à la preuve[179] qui se trouve ici mis en concurrence avec le principe d'inviolabilité des correspondances découlant du droit au respect de la vie privée[180]. En l'espèce, une lettre obtenue de manière licite a été produite en justice sans autorisation de son auteur en vue d'apporter la preuve

[177] Cass., soc., 2 octobre 2001, *pourvoi* n° 99-42.942.
[178] Cass. 1ère civ., 5 avril 2012, *pourvoi* n°11-14.177.
[179] Sur cette notion, voir A. Bergaud, *Le droit à la preuve*, préf. J.C. Saint-Pau, LGDJ, 2010.
[180] La Cour de cassation rappelle dans le premier moyen *« qu'une atteinte à la vie privée peut être justifiée par l'exigence de la protection des droits de la défense qui confère à la partie alléguant un fait le droit d'en rapporter la preuve »*. La Cour va considérer que les juges du fond auraient du rechercher si la production de ladite lettre n'était pas nécessaire à l'exercice du droit à la preuve. La Cour d'appel avait fondé sa décision sur la violation du droit au respect de la vie privée duquel découle le droit au secret des correspondances. Elle avait retenue que la lettre n'avait pas été obtenue de façon déloyale mais que le droit au respect de la vie privée avait été violé.

d'une donation immobilière rapportable à une succession. Ce document, sans en avoir le détail, comporte nécessairement plusieurs données à caractère personnel permettant d'en identifier les protagonistes[181]. Il n'est à l'époque pas fait directement référence aux données à caractère personnel mais au droit au respect de la vie privée. La Cour d'appel ayant écarté cette lettre, la Cour de cassation considère que cette dernière aurait préalablement du regarder s'il n'était pas nécessaire et proportionné de la verser aux débats[182]. Elle appliquera la même solution dans un arrêt du 25 février 2016[183].

62. Atténuations en droit de la famille – Le domaine du droit de la famille et notamment celui du divorce soulève régulièrement des questions relatives aux preuves versées au débat. Il s'agit souvent d'apporter la preuve de la faute de l'autre partie notamment en cas d'adultère ou de violences. Dans cette matière, il existe une atténuation au principe d'inviolabilité des correspondances qui permet de présenter un écrit sans le consentement de son auteur. Très clairement, le contentieux du divorce laisse prédominer le droit à la preuve. Ainsi, la faute invoquée peut être prouvée par tout mode de preuve, la seule limite étant la preuve qui serait obtenue par violence ou fraude[184]. Il en ressort un très vaste panel de modes de preuve à disposition de la partie qui entend prouver la faute. Il peut s'agir de produire un écrit papier (par exemple il est admis de verser au débat un journal intime), d'un écrit numérique, d'images captées ou alors de constatations réalisées par le biais de filatures. Dans un arrêt du 6 mai 1999, la Cour de cassation admet la production devant les juges du fond du journal intime de l'épouse, et ce quand bien même ce dernier lui aurait été subtilisé[185]. Ces exemples démontrent bien qu'en matière civile et notamment en droit de la famille, le droit à la preuve permet de produire librement des correspondances, et par la même des données personnelles, à l'appui de ses prétentions.

2° Le principe de légalité en matière de captation d'images

[181] Noms, prénoms…

[182] J. Hauser, Limites du droit au respect de la vie privée et familiale et droit à la preuve, *RTD civ*. 2012, p. 506. G. Lardeux, *Du droit de la preuve au droit à la preuve*, Dalloz, 2012, p.1596.

[183] Cass. 1ère civ., 25 février 2016, *pourvoi* n°15-12.403. J.C. Saint Pau, Droit à la preuve versus droit au respect de la vie privée, *Dalloz* 2016, p.884.

[184] Art. 259 et 259-1 du code civil.
Par exemple, Cass., 2e civ., 29 janvier 1997, *pourvoi* n° 95-15.255.

[185] Cass. civ. 1ère, 6 mai 1999, *pourvoi* n°97-12.437.
A. Lepage, *Droits de la personnalité et nécessité de la preuve*, Répertoire de droit civil, Dalloz, septembre 2009 (actualisé en juillet 2019), n°291.

63. La légalité de la collecte de données probatoires par la captation d'images par un détective privé – La question de la captation d'images à but probatoire se pose nécessairement dans le cas du recours à un détective privé. La question sous jacente est celle de la légalité du recours à un détective privé afin d'obtenir des images et rapports à vocation probatoire. Sans surprise, la Cour de cassation rappelle que le recours à de telles pratiques est licite s'il ne porte pas au droit au respect de la vie privée une atteinte excessive et s'il est justifié et proportionné au but recherché[186]. La Cour de cassation a eu à se prononcer sur la légalité de telles pratiques en matière de divorce. En effet, il est fréquent que la preuve de la faute soit rapportée par le biais de rapports dressés par un détective privé. La Cour de cassation admet le recours à cette pratique dans le cadre d'une procédure de divorce à condition qu'elle ne porte pas une atteinte excessive au droit au respect de la vie privée[187].

64. La légalité de la collecte de données probatoires par l'usage de drones – Une loi du 24 octobre 2016 est venue règlementer l'usage des drones les classant dans la catégorie des aéronefs[188]. S'agissant de l'usage privé qui peut être fait des drones, l'article L.6211-3 du code des transports pose le principe selon lequel l'usage des drones civils ne peut porter atteinte au droit de propriété. Le drone muni d'une camera permet en soit le traitement de données personnelles qui suppose, par principe, le consentement des personnes concernées[189]. La prise de vue par drone relève des dispositions de l'article D133-10 du code de l'aviation civile, qui impose une déclaration en préfecture quinze jours avant. Cette procédure témoigne des risques et enjeux attachés à l'usage des drones équipés de caméra.

Dans son rapport annuel de 2014, la CNIL alertait sur les risques d'un usage accru des drones par les particuliers et appelait à repenser le cadre existant et à appuyer la responsabilisation des usagers. Dans le mouvement engagé au niveau européen, la CNIL suggère donc la mise en place de moyens pédagogiques visant à responsabiliser les utilisateurs de drones tout en mettant en place des moyens effectifs leur permettant, le cas échéant, de faire valoir leurs

[186] Cass. civ. 1ère, 31 octobre 2012, *pourvoi* n°11-17.476. En l'espèce, le recours au détective a été diligenté par un assureur afin de contrôler si l'état de santé d'un assuré nécessité réellement l'indemnité allouée suite à un accident.

[187] Cass. civ. 1ère, 18 mai 2005, *pourvoi* n°04-13.745 ; Cass. civ. 1 ère, 15 janvier 2014, *pourvoi* n°12-24.882. Dans ces deux arrêts, la Cour de cassation admet le recours à la filature par détective privé.
Cass. civ. 2e, 3 juin 2004, *pourvoi* n°02-19.886. La Cour de cassation rejette le rapport établi au motif que la durée importante de la filature portait une atteinte excessive au droit au respect de la vie privée ; Cass. civ. 1ère, 22 septembre 2001, *pourvoi* n°15-24.015. La Cour de cassation considère que *« l'immixtion dans la vie privée excédait les nécessités de l'enquête »*.
A.E. Credeville, *Vérité et loyauté des preuves*, Rapport 2004, Cour de cassation.

[188] Loi n° 2016-1428 du 24 octobre 2016 relative au renforcement de la sécurité de l'usage des drones civils.

[189] C. Rotily, L. Archambault, Drones civils professionnels et RGPD : enjeux liés à la collecte des données personnelles et au respect de la vie privée, *Dalloz IP/IT*, 2019, 376.

droits en cas d'atteintes aux libertés fondamentales. En 2015, le Parlement européen suggérait la réalisation d'une analyse d'impacts et la mise en place d'une meilleure information des usagers sur une utilisation « responsable » des drones[190].

Un usage au sein de l'entreprise nécessite, comme tout moyen de surveillance, une information des salariés conformément à l'article 37 du règlement générale sur la protection des données[191].

Encore récemment considéré comme un « ovni juridique » le drone soulève encore aujourd'hui des interrogations auxquelles les juges sont venus apporter d'utiles précisions.

Récemment, un arrêt de la Cour d'appel de Paris[192] a apporté un regard nouveau sur cet équilibre précaire entre respect de la vie privée et droit à la preuve s'agissant d'images captées par un drone et versées au débat dans un litige en matière d'urbanisme. Dans cet arrêt, la Cour d'appel rejette les images captées par le drone aux motifs qu'elles n'étaient pas nécessaires et que l'atteinte n'était pas proportionnée[193]. Si le débat ne portait pas précisément sur ce point, l'arrêt soulève indirectement la question du recueil de données par de nouveaux moyens liés aux évolutions technologiques à disposition des individus. La question étant de savoir dans quelle mesure il est possible pour un individu de recourir à l'utilisation d'un tel dispositif dans le but de recueillir des données utiles à l'appui de ses prétentions ?

Le Conseil d'Etat a aussi eu l'occasion d'apporter des précisions sur l'usage des drones comme moyen de collecte de données probatoires. Dans le cadre des dispositions prises face à la pandémie de 2019, la préfecture de Paris avait décidé de recourir à l'usage de drones afin de contrôler les rassemblements publics éventuels de personnes au delà de la jauge autorisée. Les images captées étaient transmises en temps réel aux services de la préfecture. Le tribunal administratif a écarté le qualificatif de traitement de données à caractère personnel considérant d'une part que le dispositif ne visait pas la collecte de données identifiantes écartant donc l'application du règlement général sur la protection des données et d'autre part l'usage prévu était « légitime ». Il faut rappeler que ces mesures étaient prises dans le cadre de l'état d'urgence sanitaire qui permet la mise en œuvre de mesures plus attentatoires aux libertés mais devant être proportionnées au but. Néanmoins par ordonnance du 18 mai 2020, le Conseil d'Etat a considéré qu' « il est constant qu'un usage du dispositif de surveillance par

---

[190] Rapport du Parlement européen, *« Les conséquences de l'usage civil des drones sur la protection de la vie privée et des données à caractère personnel »*, 2015. Sur le sujet voir, C. Féral-Schuhl, *Cyberdroit, Le droit à l'épreuve de l'internet*, Dalloz, 8e ed., 2020/2021.

[191] V. *infra* n°65.

[192] CA Paris, pôle 1, ch. 3, 15 mai 2019, n°18/26775.

[193] C. Bléry, *Droit à la preuve : nouvelle pierre à l'édifice jurisprudentiel à propos d'un constat par drone, Dalloz Actualité*, 3 septembre 2019.

drone effectué conformément à la doctrine d'emploi fixée par la note du 14 mai 2020 n'est pas de nature à porter, par lui-même, une atteinte grave et manifestement illégale aux libertés fondamentales invoquées »[194]. En l'espèce les capacités des drones utilisés permettant notamment d'effectuer des zooms et donc l'identification des individus, ils doivent être considérés comme des moyens de collecte de données à caractère personnel. Ainsi au vu des dispositions de la loi informatique et libertés et de la directive Police-Justice[195], ces procédés doivent être analysés comme des traitements de données à caractère personnel et doivent donc reposer sur un texte réglementaire notamment au vu des atteintes potentielles pour la vie privée. Le Conseil d'Etat choisit donc de raisonner davantage en fonction des possibilités offertes par les drones qu'en fonction de l'usage qui en est réellement fait[196].

On peut s'interroger sur l'application de la directive Police-Justice qui, par principe, s'applique aux traitements de données pénales. Toutefois son article premier laisse sous-entendre une portée plus large dont il découle que la police administrative ayant une mission de prévention des infractions, la directive tend à s'appliquer. En effet l'article premier vise « les autorités compétentes » en matière de prévention des infractions[197].

S'agissant de l'usage de drones par les autorités, la CNIL a prononcé une sanction à l'encontre du ministère de l'Intérieur dans une délibération en date du 12 janvier 2021 sur le fondement d'un manquement à l'obligation de licéité et pour manquement à l'obligation de réaliser une étude d'impact. Les données concernées étant potentiellement des données sensibles au sens de la loi informatique et libertés, le traitement doit être encadré par des dispositions législatives et faire l'objet d'une étude d'impact en application des articles 89 et 90 de cette même loi. La Commission retient que la capacité des cameras de haute résolution rend possible l'identification des individus, entrainant un risque important en termes de libertés, aucun dispositif de floutage n'étant à ce jour effectif[198]. La proposition de loi « sécurité globale » dans son article 22 vise à intégrer au sein du code de la sécurité intérieure

[194] CE, 18 mai 2020, n° 440442, 14.
[195] Art. 3 de la directive du 27 avril 2016.
[196] X. Bioy, Les drones produisent-ils des données personnelles ? *AJDA*, 2020, 1552. M.C. Montecler, Il faut une loi sur l'usage des drones par la police, *AJDA*, 2020, 2235.
[197] L'article premier de la directive police-Justice du 2 avril 2016 dispose que « La présente directive établit des règles 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 menaces pour la sécurité publique et la prévention de telles menaces ».
[198] Délibération CNIL SAN-2021-003 du 12 janvier 2021. La CNIL a prononcé un rappel à l'ordre et une injonction de mise en conformité. La Commission invoquait aussi le manquement à l'obligation de mettre à dispositions certaines informations tel que le responsable du traitement, la finalité du traitement ainsi que le droit d'accès et de rectification des données.

des dispositions relatives à l'usage des caméras aéroportées par les autorités[199]. Cette nécessité d'encadrer le recours à ces dispositifs est depuis longtemps suggérée par la CNIL. Ces dispositions viennent donc poser un cadre à l'usage des drones par les autorités visant la captation d'images en temps réel. Elles précisent notamment que les dispositifs ne peuvent assurer une surveillance permanente et ne peuvent pas capter les images dans les domiciles. La proposition de loi mentionne que les autorités concourant à la sécurité intérieure et à la défense nationale dans leur mission notamment de prévention, constatation et poursuite des infractions pénales, peuvent recourir au dispositif de caméras aéroportées, notamment pour collecter des preuves. La CNIL appelle néanmoins à fixer des garanties supplémentaires et notamment à limiter davantage les finalités de tels traitements[200].

3°La légalité dans la collecte de preuve dans l'entreprise

65. Dispositions générales – Le code du travail dispose que *« Nul ne peut apporter aux droits des personnes et aux libertés individuelles et collectives de restrictions qui ne seraient pas justifiées par la nature de la tâche à accomplir ni proportionnées au but recherché »*[201], aussi, *« aucune information concernant personnellement un salarié ne peut être collectée par un dispositif qui n'a pas été porté préalablement à sa connaissance »*[202]. Le contentieux relatif à la preuve de la faute en droit du travail est vaste. Il existe une importante jurisprudence en la matière qui s'est attachée à trouver un juste équilibre entre les droits de l'employeur et ceux du salarié sur fond de ce qu'on a coutume d'appeler la « vie privée au travail »[203]. La question est de savoir dans quelle mesure un employeur peut opérer une certaine surveillance de ses salariés sur leur lieu de travail et produire les informations recueillies dans un éventuel litige. Après le célèbre arrêt de principe « Nikon » du 2 octobre 2001 qui proclama l'existence d'un droit au respect de la vie privée du salarié et plus précisément le droit au secret de ses correspondances « personnelles » conservées sur son ordinateur professionnel, la Cour de cassation va venir

[199] Proposition de loi n° 3452, du 20 octobre 2020 relative à la sécurité globale.
[200] Délibération CNIL n° 2021-011 du 26 janvier 2021 portant avis sur une proposition de loi relative à la sécurité globale (demande d'avis 20020769).
[201] Art. L1121-1 du code du travail.
[202] Art. L1222-4 du code du travail.
[203] Cette notion de droit au respect de sa vie privée sur son lieu de travail est issue de l'arrêt de principe « Nikon » de la Cour de cassation en date du 2 octobre 2001. Cass. soc., 2 octobre 2001, *pourvoi* n°99-42.942. Par cet arrêt, la Cour de cassation consacre le droit au respect de sa vie privée sur son lieu de travail, interdisant ainsi à l'employeur l'accès aux messages personnels de ses salariés à la condition que ces messages soient clairement indiqués comme étant « personnels » et quand bien même ces derniers seraient conservés sur le disque dur de l'ordinateur de l'entreprise.
P. Langlois, Courrier électronique et vie privée au travail, *Dalloz*, 2001, p. 3286.

préciser les contours de cette notion de vie privée au travail. Après avoir affirmé l'existence d'une présomption de la nature professionnelle des messages contenus sur l'ordinateur mis à disposition par l'employeur[204], la Cour de cassation va quelque peu revoir sa position en autorisant l'accès par l'employeur à toutes les données contenues dans les ordinateurs professionnels de ses salariés en leur présence[205]. Cette présomption vaut également pour les « SMS » envoyés et reçus par un salarié sur le téléphone portable mis à disposition par l'employeur[206]. La Cour de cassation a par la suite étendu cette présomption à tout message qui serait conservé sur l'ordinateur du salarié mis à disposition par l'entreprise quand bien même il serait issu de la messagerie personnelle de ce dernier[207] pour semble t-il revenir sur cette conception dans un arrêt récent en 2016[208] dans lequel elle affirme la distinction qui doit être faite entre messages issus de la messagerie professionnelle et messages issus de la messagerie personnelle du salarié. Ainsi, les messages issus de la messagerie personnelle du salarié, quand bien même ils seraient conservés sur l'ordinateur mis à disposition par l'employeur, ne peuvent pas être produits en justice par l'employeur dans le but éventuel d'apporter la preuve d'une faute commise par le salarié.

Cet arrêt intervient quelques jours après l'arrêt de la Cour européenne des droits de l'homme *Barbulescu c/ Roumanie* du 12 janvier 2016[209] qui autorise l'employeur à enregistrer une conversation issue de la messagerie professionnelle d'un salarié afin de l'utiliser comme preuve d'une faute commise par ce dernier en ayant recours à un logiciel espion. Dans cette affaire, la grande chambre s'est prononcée le 5 septembre 2017[210]. La Cour européenne des droits de l'homme est venue préciser les conditions de licéité d'une telle surveillance dont la mise en œuvre est subordonnée à celle de garanties adéquates et suffisantes. L'employeur doit notamment avertir le salarié du recours à de telles pratiques de surveillance qui doivent être justifiées et adaptées. Sur la question, le droit interne semble être en accord avec la jurisprudence de la Cour européenne des droits de l'homme puisque les dispositions de l'article L1222-4[211] du code du travail prévoient que soit informé le salarié de toute collecte

[204] Cass. soc., 18 oct. 2006, *pourvoi* n°04-48.025.
[205] Cass. soc., 17 juin 2009, *pourvoi* n°08-40.274.
[206] Cass. com., 10 février 2015, *pourvoi* n°13-14.779.
[207] Cass. soc. 19 juin 2013, *pourvoi* n°12-12.138.
[208] Cass. soc. 26 janvier 2016, *pourvoi* n°14-15.360.
[209] Cour E.D.H., *Barbulescu c/ Roumanie,* 12 janvier 2016, *requête* n°61496/08.
J. P. Marguénaud, *Conv. EDH, art 8 : vie privée,* Répertoire de droit européen, Dalloz, octobre 2017, n°58.
P. Adam, Droit (de l'employeur)à la preuve et vie privée(du salarié), *Dalloz*, 2016, p.211.
[210] Cour E.D.H., gr. ch. *Barbulescu c/ Roumanie,* 5 septembre 2017, *requête n*°61496/08.
[211] Art. L1222-4 du code du travail *« Aucune information concernant personnellement un salarié ne peut être collectée par un dispositif qui n'a pas été porté préalablement à sa connaissance. »*

d'informations personnelles le concernant. Aussi l'article L.2312-38[212] du code du travail prévoit que soit informé, au préalable, le comité social et économique[213] de toute mise en œuvre dans une entreprise de moyens de surveillance de l'activité des salariés.

66. La collecte de données personnelles conservées sur les outils mis à disposition par l'employeur – La Cour européenne des droits de l'Homme a eu de nouveau à se prononcer sur la question d'une éventuelle violation des dispositions de l'article 8 dans un arrêt du 22 février 2018 *Libert c/ France*[214]. La Cour va néanmoins conclure à une ingérence proportionnée dans la vie privée du salarié licencié pour avoir usé de l'outil informatique mis à disposition par son employeur à des fins personnelles. Cette utilisation a été mise à jour suite à la découverte de données accablantes enregistrées sur l'ordinateur sur le disque D/ renommé « données personnelles ». Faisant écho à la jurisprudence antérieure (notamment l'arrêt Nikon), la question se pose alors du droit d'accès de l'employeur à ce fichier renommé « données personnelles ». La Cour européenne des droits de l'homme va considérer que le fait de renommer l'intégralité du disque dur (par défaut intitulé « données ») « données personnelles » ne suffit pas à caractériser sa nature « privée »[215]. Elle rejoint sur ce point le raisonnement adopté par la Cour de cassation. Cet arrêt est intéressant à de nombreux égards, notamment parce qu'il n'est fait à aucun moment référence aux textes relatifs aux données à caractère personnel (contrairement à la jurisprudence *Barbulescu* qui prend soin de rappeler les dispositions applicables en la matière[216]). Ensuite, il soulève malgré tout des interrogations quand à la terminologie utilisée pour justifier cette ingérence. Outre le fait que tout le disque D/ ait été renommé, la mention « personnelles » ne suffisait elle pas à rendre ce fichier privé ? La Cour fonde ici son raisonnement sur une ingérence justifiée, proportionnée et légitime de

[212] Art. L2312-38 al. 3 du code du travail *« Le comité est informé et consulté, préalablement à la décision de mise en œuvre dans l'entreprise, sur les moyens ou les techniques permettant un contrôle de l'activité des salariés. »*

[213] Les comités sociaux et économiques ont été créés au 1er janvier 2018 par les ordonnances du 22 septembre 2017 et fusionnent toutes les instances représentatives des salariés dans les entreprises d'au moins 11 salariés.

[214] Cour E.D.H., 5e sect., *Libert c/ France*, 22 février 2018, *requête* n°588/13.

[215] En référence au règlement intérieur applicable dans l'entreprise qui précise que les données stockées sur les ordinateurs mis à disposition par l'employeur doivent être strictement identifiées comme « privé » pour ne pas être présumées professionnelles.

[216] Notamment la recommandation du Comité des ministres au Etats membres du 1er avril 2015 qui prône une transparence en matière de surveillance des salariés de l'utilisation faite d'internet au travail, ainsi qu'une nécessité de tout contrôle opéré par l'employeur. La recommandation appelle à la mise en œuvre de « mesures préventives » plus que punitives (point 14). L'arrêt fait également référence à l'avis 8/2001 du groupe de travail sur la protection des données qui appelle à *«une réponse proportionnée de l'employeur aux risques qu'il encourt de porter atteinte à la vie privée légitime et autres intérêts des salariés ».*

l'employeur au vu de l'article 8 de la convention et sur une violation du règlement intérieur par le salarié.

Récemment, la chambre sociale de la Cour de cassation a apporté des précisions quant à la portée de la légalité dans la collecte de données probatoires dans l'entreprise. Dans un arrêt du 25 novembre 2020, la Cour de cassation réaffirme que les adresses IP sont des données identifiantes et donc des données à caractère personnel au sens de la loi informatique et libertés[217]. Aussi, l'exploitation d'un fichier de journalisation permettant par recoupement de contrôler l'activité des salariés de manière indépendante constitue un traitement de données à caractère personnel et doit donc faire l'objet d'une déclaration préalable. L'intérêt de cet arrêt réside dans le fait que la Cour de cassation ne rejette pas pour autant la preuve collectée de manière illicite. Au regard du droit à la preuve et d'un contrôle de proportionnalité, la Cour de cassation considère que le moyen peut être retenu s'il est « indispensable » à l'exercice du droit[218].

67. La collecte de données par géolocalisation des salariés – La question de la surveillance des salariés au travail a été soulevée par celle de l'utilisation de moyens de géolocalisation par l'employeur afin de contrôler le temps effectif de travail. Dans une délibération du 16 mars 2006[219], la CNIL avait fait le constat d'une augmentation de l'utilisation de dispositifs de géolocalisation par les employeurs. Elle émet alors des recommandations concernant ces procédés précisant qu'ils devraient seulement être utilisés soit dans un but de sureté ou de sécurité du salarié, soit dans certaines professions pour lesquelles ce traitement est nécessaire (taxi, urgences…), soit lorsqu'ils constituent le seul moyen de contrôler le temps de travail. Aussi, la commission rappelle que *« l'utilisation d'un dispositif de géolocalisation ne doit pas conduire à un contrôle permanent de l'employé concerné »*. L'utilisation d'un tel dispositif doit être portée à la connaissance du salarié concerné et doit être envisagée pour les finalités définies initialement[220]. La géolocalisation des salariés a soulevé de nombreux contentieux notamment sur le fondement de la déloyauté[221].

---

[217] Reprenant ici, Cass., civ. 1ère, 3 novembre 2016, *pourvoi* n° 15-22.595.

[218] Cass., soc., 25 novembre 2020, *pourvoi* n°17-19.523.

[219] Délibération CNIL 2006-066 du 16 mars 2006 portant adoption d'une recommandation relative à la mise en œuvre de dispositifs destinés à géolocaliser les véhicules automobiles utilisés par les employés d'un organisme privé ou public.

[220] Cass. soc. 3 novembre 2001, *pourvoi* n°10-18.036. Dans cet arrêt antérieur au RGPD, la Cour de cassation fait également référence à l'obligation pour l'employeur de déclarer la mise en œuvre du dispositif à la CNIL.
Cass. soc. 19 décembre 2018, *pourvoi* n°17-14.631. La Cour de cassation rappelle que le dispositif mis en œuvre dans le but de contrôler le temps de travail effectif d'un salarié ne peut l'être qui s'il constitue l'unique moyen d'effectuer un tel contrôle.

[221] V. *infra* n°85 s.

68. La collecte de données par le recours à la vidéosurveillance des salariés – Concernant la surveillance par caméra, là aussi, en vertu des articles précités[222] le Comité social et économique ainsi que les salariés doivent être informés au préalable du recours à ce dispositif. L'employeur n'a plus à déclarer l'installation du dispositif à la CNIL. Pour se conformer au règlement général sur la protection des données, il doit clairement indiquer par panneaux d'affichage la présence des cameras ainsi que le nom du responsable du traitement, la durée de conservation des données[223] recueillies ainsi que l'existence d'un droit d'accès. En termes de preuve, la question sous jacente est celle de l'utilisation par l'employeur des données recueillies via le système de vidéosurveillance. La Cour de cassation a rappelé récemment que l'admissibilité des preuves recueillies est attachée à la licéité du système de surveillance. L'employeur ne peut pas fournir comme preuve des images tirées d'enregistrement de vidéosurveillance dont les salariés n'auraient pas eu connaissance[224]. Venant limiter la portée de l'arrêt *Barbulescu*, la Cour européenne des droits de l'Homme dans un arrêt du 17 octobre 2019, a confirmé la conception large de la notion de vie privée avec une application sur le lieu de travail. S'agissant du recours par l'employeur à un moyen de surveillance secret des salariés, elle considère qu'il peut être justifié par un impératif prépondérant qui repose en l'espèce sur des « soupçons raisonnables »[225].
Si le droit au respect de la vie privée constitue une limite évidente à la liberté de la preuve, le principe de sauvegarde dignité humaine en constitue une seconde.

B. La collecte de données personnelles à vocation probatoire confrontée au principe de sauvegarde de la dignité humaine

69. Dignité humaine – Le principe de respect de la dignité humaine issue de la Déclaration des droits de l'Homme de 1789 a trouvé un écho notamment dans la jurisprudence relative aux lois bioéthiques. Sans reprendre l'historique de cette consécration, il faut noter qu'en matière de collecte de preuves, la dignité humaine trouve à s'appliquer s'agissant des procédés utilisant des techniques invasives. La prohibition de toute atteinte à la dignité humaine dans la collecte de données à vocation probatoire (1°) soulève une réflexion

[222] Art. L1222-4 et L2312-38 al. 3 du code du travail.
[223] La durée de conservation des données est fixée par l'employeur.
[224] Cass. soc. 20 septembre 2018, *pourvoi* n°16-26.482.
[225] Cour E.D.H., 17 octobre 2019, Lopez Ribalda et a c/ Espagne, n° 1874/13 et n° 8567/13. G. Loiseau, Droits de la personnalité, *Légipresse*, 2020, p. 64. L. Burgorgue-Larsen, Actualité de la convention européenne des droits de l'Homme, *AJDA*, 2020, p. 160.

particulière sur la place du consentement dans les actes de collecte des données probatoires (2°).

1° La prohibition de toute atteinte à la dignité humaine dans la collecte de données à vocation probatoire

70. Prohibition absolue – Le recours à toute forme de violence dans le recueil de preuves est prohibé et ce principe ne connait aucune exception. Ce principe pose par exemple l'interdiction du recours à tout procédé scientifique visant à obtenir des aveux et tout recours à la violence physique et morale peu importe l'infraction commise. Cela a été rappelé par la Cour européenne des droits de l'Homme dans différents arrêts, qui ont condamné certaines pratiques sur le fondement de l'article 3 de la Convention européenne des droits de l'Homme[226].

71. Prohibition du recours à des procédés scientifiques visant l'obtention d'aveux – Parmi les procédés de recueil de preuves strictement prohibés au nom du principe de dignité on peut également citer le recours à l'injection de produits (sérums de vérité) ou les procédés scientifiques tel que le polygraphe (détecteur de mensonge). Ces procédés sont interdits au motif d'une atteinte à la dignité mais aussi du fait de l'absence de fiabilité et aussi pour l'atteinte évidente au droit de se taire.

72. Prohibition du recours à la violence dans la collecte de données probatoires – Le principe de légalité dans le recueil de preuves trouve particulièrement à s'appliquer s'agissant des méthodes d'interrogatoire. La jurisprudence interne, sous l'influence certaine des arrêts de la Cour européenne des droits de l'Homme, a pu préciser cette application de la légalité. Par exemple, s'agissant de la collecte de données probatoires lors des interrogatoires les juges ont très tôt condamné le recours à toute violence physique ou morale ou mauvais traitement[227].

[226] Par exemple, Cour E.D.H 18 janvier 1978 Irlande c/ Royaume-Uni, req. n° 5310/71, Cour E.D.H. 18 octobre 2001, *Indelicato c/ Italie*, req. n° 31143/96 , Cour E.D.H., 4 novembre 2010, *Darraj c/ France*, req. n° 34588/07, Cour E.D.HH, gr. ch., 11 juillet 2006, *Jalloh c/ Allemagne*, req.n° 54810/00. J. Buisson, *Preuve*, Répertoire de droit pénal et de procédure pénale, Dalloz, *op. cit.*

[227] Cass., crim., 18 février 1954, D. 1954, Cour E.DH.,H, gr. ch., 11 juillet 2006, *Jalloh c/ Allemagne*, req. n° 54810/00. Cour E.D.H., 4 décembre 1995, *Ribitsch c/Autrich*e, req. n° 18896/91 et Cour E.D.H. 27 août 1992, *Tomasi c/ France*,req. n° 12850/87 (précisent que cette prohibition s'applique aux actes de violences illégitimes commis par les forces de l'ordre dans l'exercice de leurs fonctions.

Cette prohibition de tout procédé qui porterait atteinte à la dignité de la personne soulève, s'agissant de la collecte de preuves, la question de la place du consentement dans les actes réalisés.

2° Réflexion quant à la place du consentement dans les actes de collecte de données probatoires

73. La place du consentement dans la collecte de données à vocation probatoire – Par extension, l'analyse de la légalité dans la collecte de données probatoires soulève, sous couvert de respect de la dignité humaine, d'inviolabilité du corps humain, de vie privée et d'intégrité, la question de la place du consentement des individus s'agissant des prélèvements biologiques réalisés sur leur personne. Cette question très transversale aurait pu trouver sa place dans le raisonnement consacré à la vie privée, toutefois le caractère intrusif de certains actes de recueil qui pourrait être réalisés sous contrainte renvoie aux questions de dignité et d'intégrité du corps humain. Le consentement constitue une des bases légales permettant le traitement de données à caractère personnel. Il est évident que s'agissant de la collecte de données à vocation probatoire visant la lutte contre les infractions, le traitement repose sur une base légale autre que le consentement attachée précisément à la nature et à la finalité de celui-ci. Néanmoins, on peut s'interroger, dans une présentation non exhaustive, sur la place du consentement s'agissant d'actes intrusifs qui dans un contexte différent ne pourraient être réalisés sans le consentement de l'intéressé, renvoyant ici à ce qui peut être désigné en matière pénale sous le vocable de « contrainte probatoire »[228]. La question du consentement à la collecte trouve également à se poser en matière civile mais nécessite d'aborder séparément les deux contentieux.

74. Le consentement aux prélèvements biologiques en matière civile – En matière civile, les mesures de prélèvement biologiques se rencontrent essentiellement en matière de filiation avec le recours aux tests ADN dans les procédures visant à établir ou faire reconnaitre une filiation[229]. Cette procédure ne peut être ordonnée que par un juge et avec le consentement de l'intéressé[230]. L'article 16-10 du code civil encadre cette pratique et fait suite à la loi

[228] Pour reprendre les termes de Jacques Buisson, *Preuve*, Répertoire de droit pénal et de procédure pénale, *op. cit.*, 209. Voir sur le sujet, C. Copain, *L'encadrement de la contrainte probatoire en procédure pénale française*, Thèse de doctorat, droit, Université Lyon 3, 2011, 633 p.
[229] J. Hauser, La preuve biologique, reine des preuves ?, *RTD civ.*, 1993, p. 811.
[230] Art. 16-10 à 16-13 du code civil.

bioéthique du 29 juillet 1994[231]. Ainsi, le législateur réserve le recours aux tests ADN aux motifs médicaux ou scientifiques et impose que le consentement de la personne concernée soit recueilli par écrit.

La preuve ADN est devenue incontournable en droit de la filiation[232]. Depuis un arrêt du 28 mars 2000, la jurisprudence reconnait que le recours à l'expertise biologique est de droit pour les parties, sauf s'il existe un motif légitime[233]. Ce revirement a pu être assimilé à la reconnaissance d'un « droit à la preuve biologique »[234]. Toutefois, si le recours à l'expertise biologique est de droit pour les requérants, le juge ne pouvant sauf exception s'y opposer, cela ne signifie pas pour autant que le prélèvement peut être fait sous la contrainte. Les articles 16-10 et 16-11 du code civil visent le consentement « exprès » de la personne, nécessaire donc à tout acte visant un prélèvement biologique.

Le recours au test ADN dans le contentieux de la filiation a toujours divisé et fait l'objet, encore aujourd'hui, de controverses opposant notamment les juridictions internes et supra nationales. L'article 16-11 alinéa 5 du code civil dispose que les tests ADN ne peuvent être réalisés sur un défunt sauf si son accord avait été donné de son vivant. Cette position a été confirmée par le Conseil Constitutionnel dans une décision du 30 septembre 2011[235] au nom du respect dû aux morts. Le Conseil constitutionnel affirme donc qu'il ne peut être recouru à de tels tests sans le consentement de l'intéressé.

La Cour européenne des droits de l'homme a, quant à elle, tranché en ce sens dans un arrêt du 16 juin 2011[236] par lequel elle condamne la France pour violation de l'article 8. Dans cette affaire, la Cour européenne des droits de l'homme a fait primer l'intérêt de l'enfant à connaitre ses origines au nom du droit au respect de sa vie privée[237]. C'est au nom de cet intérêt que la Cour européenne des droits de l'homme a maintenu une filiation paternelle quand bien même celle-ci ne reflétait pas la réalité biologique[238]. En l'espèce, bien que l'ADN ait apporté la preuve de l'absence de lien de filiation, la Cour EDH a préféré maintenir ce lien,

---

[231] Loi n°96-653 du 29 juillet 1994 relative au respect du corps humain.

[232] Cass. civ. 1ère, 28 nov. 2012, n°11-23.170 ; Cass. civ. 1ère, 14 janvier 2015, n°13-28.256.

[233] Cass., civ. 1ère, 28 mars 2000, pourvoi n° 98-12.806.

[234] F. Ferrand, *Preuve. Le juge et les techniques biologiques modernes*, Répertoire de procédure civile, Dalloz, décembre 2013, actualisation décembre 2019.

[235] Cons. Const., décision n°2011-173 QPC du 30 septembre 2011.

[236] Cour E.D.H., *Pascaud c/ France*, 16 juin 2011, 19535/08.

[237] Le requérant ne disposant pas d'autres moyens de faire établir la filiation et le test ADN constituant une « preuve déterminante » de celle-ci.

L. Milano, Droit d'établir sa filiation biologique et consentement aux tests ADN, *JCP G*, 2011, n°27.

J. Hauser, Le droit à l'expertise biologique et la Convention EDH : la vérité biologique à tout moment ?,*RTD civ.* 2011, p. 526.

[238] Cour E.D.H., 18 février 2014, *A.L. c/ Pologne*, n°28609-08. Cour EDH, 18 février 2014, , *Ostace c/ Roumanie*, n°12547/06.

ce qui pose ici la question de la force probante de l'ADN[239]. Ainsi, *« la filiation ne se résume pas à la seule transmission des gènes »*[240]. La réalisation de tels tests est basée sur le consentement mais le refus de se soumettre à un test ADN peut avoir des conséquences, puisque le juge peut tirer toutes les conclusions de ce refus[241]. Récemment pourtant, la Cour européenne des droits de l'homme a estimé que le fait pour des juges d'ordonner à un individu de se soumettre à un test ADN ne viole pas le droit au respect de la vie privée[242]. La Cour de cassation opère également à ce sujet un contrôle de proportionnalité entre les intérêts en présence et notamment entre l'application des délais légaux de prescription et le droit au respect de la vie privée. Il s'agissait en l'espèce d'une action intentée en reconnaissance paternité. Par le jeu des prescriptions, cette dernière n'était par principe pas recevable. Toutefois, la Cour de cassation a choisi d'écarter l'application des seules règles de prescription au profit d'un contrôle de proportionnalité sur le fondement de la vie privée. Plus précisément, la Cour de cassation observe si l'application des délais de prescription ne portait pas une atteinte excessive au droit au respect de la vie privée[243].

L'utilisation de l'ADN comme mode de preuve trouve également à s'appliquer en procédure pénale et soulève là aussi grand nombre d'interrogations.

75. Le consentement aux prélèvements biologiques en matière pénale – Dans le cadre d'une enquête ou d'une information judiciaire, il peut être procédé à des prélèvements externes dans le but de collecter des données utiles. L'article 55-1 du code de procédure pénale prévoit les dispositions relatives à cette collecte et précise que toute opposition à l'acte par une personne à l'encontre de laquelle il existe des raisons plausibles de soupçonner qu'elle a commis ou tenté de commettre une infraction est punie d'un an d'emprisonnement et 15000 euros d'amende. S'agissant de prélèvements internes, la question de la légalité sur fond

[239] V.*infra* n°118 s.
[240] E. Viganotti, Filiation : deux décisions intéressantes de la CEDH, *AJ Famille*, 2014, p. 246.
[241] Art. 11 du code de procédure civile.
[242] Cour EDH, 29 janvier 2019, n°62257/15, Mifsud c/ Malte.
M. Saulier, Droit à une filiation vs droit au respect de la vie privée du père : y a-t-il vraiment encore un débat ?, *AJ Famille*, 2019, p. 155.
A.M. Leroyer, Expertise en matière de filiation : une question d'identité, *RTD civ.*, 2019, p. 305.
[243] Cass, civ., 1ère, 7 novembre 2018, n°17-25.938 ; Cass., civ., 1ère, 21 novembre 2018, n°17-21.095. La Cour de cassation opère alors un contrôle de proportionnalité et prend le soin de détailler la manière de la réaliser en observant d'abord le droit menacé et la légitimité du but recherché. Bien que la « pédagogie » de la Cour ait ici été saluée, la décision prise a toutefois fait l'objet de critiques.
L. Mauger-Vielpeau, La filiation paternelle à l'épreuve du contrôle de proportionnalité, *Dalloz*, 2019, p. 207.
P.Y. Gautier, La prescription sur le billot du contrôle de proportionnalité, *Dalloz*, 2019, p.64.

de respect de la dignité trouve davantage à se poser[244]. L'article 60 du code de procédure pénale prévoit qu'il peut être fait appel à toute personne qualifiée afin de procéder à des constatations ou examens techniques ou scientifiques. Les prélèvements génétiques dans le but d'identification par l'ADN ont connu un essor considérable depuis la création du fichier national des empreintes génétiques en 2001[245]. Par la loi du 17 juin 1998[246], le législateur impose le recueil ADN s'agissant des infractions de nature sexuelle. Par la suite, plusieurs lois sont venues étendre les cas de fichage des profils ADN, cette donnée s'étant rapidement imposée comme la donnée d'identification par excellence[247].

Récemment, la Cour européenne des droits de l'Homme a rappelé qu'un prélèvement salivaire ne peut sans porter atteinte à la vie privée être réalisé sans base textuelle[248]. En droit interne, l'article 706-55 du code de procédure pénale prévoit les cas permettant le recueil de traces génétiques[249]. Aussi, l'article 706-56 du code de procédure pénale dispose que le refus de se soumettre au prélèvement est puni de un an d'emprisonnement et de 15000 euros d'amende. Le Conseil constitutionnel amené à se prononcer sur ces dispositions, à l'occasion d'une question prioritaire de constitutionalité, avait validé le dispositif[250]. Néanmoins, la Cour européenne des droits de l'Homme quant à elle a considéré que le régime en raison notamment des durées de conservation et de l'absence de droit à demander l'effacement des données, était contraire à la Convention[251]. La Cour européenne des droits de l'Homme a, par la même occasion, considéré que la sanction prononcée pour refus de se soumettre au prélèvement portait atteinte au droit au respect de la vie privée. La chambre criminelle de la Cour de cassation a rendu récemment un arrêt qui semble prendre le contre-pied de la position de la Cour européenne des droits de l'Homme en considérant que la condamnation prononcée sur le fondement du refus de se soumettre à un prélèvement ne porte pas atteinte au droit au respect de la vie privée[252]. En l'espèce, le requérant qui opposait le refus au prélèvement était poursuivi et non condamné, ce qui lui permettait de demander l'effacement des données au FNAEG. Dans un arrêt du 31 mars 2020, la chambre criminelle de la Cour de cassation considère, sur le fondement de l'article 60 du code de procédure pénale, qu'il peut être

[244] Sur le sujet voir, C. Ambroise-Castérot, Recherche et administration des preuves en procédure pénale : la quête du graal de la vérité, *AJ Pénal*, 2005, p.261.
[245] V. *infra* n°180.
[246] Loi n° 98-468 du 17 juin 1998 relative à la prévention et à la répression des infractions sexuelles ainsi qu'à la protection des mineurs.
[247] V *infra* n°118 s.
[248] Cour E.D.H., 14 avril 2020, *Dragan Petrovic c/ Serbie*, n° 75229/10.
[249] V. *infra* n°122.
[250] Cons. Const., 16 septembre 2010, n°2010-25 QPC.
[251] Cour E.D.H., 22 juin 2017, *Aycaguer c/ France*, n° 8806/12.
[252] Cass., crim., 15 janvier 2019, *pourvoi* n° 17-87.185.

procédé à un prélèvement sanguin par usage de la contrainte[253]. Les dispositions précitées semblent donc laisser, en matière pénale, peu de place au consentement.

La collecte de données probatoires doit donc respecter le cadre légal fixé et se trouve mise en concurrence avec notamment le droit au respect de la vie privée au regard du droit à la preuve. La collecte de preuves se trouve également confrontée à une exigence de loyauté. Cette notion reste toutefois ambivalente et trouve à s'appliquer différemment selon la procédure et surtout selon que l'acte émane d'une autorité publique ou non.

Section 2 : La collecte de données soumise au principe de loyauté de la preuve

76. La loyauté, un principe empreint d'ambivalence – Le sujet de l'application faite du principe de loyauté de la preuve interroge autant qu'il divise[254]. Il appelle quoi qu'il en soit à distinguer les procédures civiles et pénales qui en font une application distincte. Le principe de loyauté n'est pas strictement défini par les textes, l'idée d'une telle inscription ayant été rejetée ou abandonnée dans les deux matières. La loyauté de la preuve a été érigée par la doctrine et par la jurisprudence en principe directeur du procès, cette dernière reconnaissant le principe de loyauté comme composante des règles régissant l'administration de la preuve. Ce principe soulève aujourd'hui encore des interrogations tant sur sa définition que sur sa portée[255].

On peut retenir la définition donnée par le doyen Bouzat qui faisait référence à *« une manière d'être de la recherche des preuves, conforme au respect des droits de l'individu et à la dignité de la justice »*[256]. On trouve également des références à la « loyauté procédurale »[257] ou à la « loyauté probatoire »[258] pour désigner le principe de loyauté dans l'obtention de la preuve.

---

[253] Cass., crim., 31 mars 2020, *pourvoi* n° 19-85.756. P.J. Delage, Prélèvement sanguin contraint fondé sur l'article 60 du code de procédure pénale : une ingérence « prévue par la loi » ?, *RSC*, 2020, p. 673.

[254] O. Decima, De la loyauté de la preuve pénale et de ses composantes, *Dalloz*, 2018, p .103.

[255] Voir le rapport de la Cour de cassation, P. Lemoine, La loyauté de la preuve à travers quelques arrêts récents de la chambre criminelle, 2004.
W. Azoulay, Loyauté de la preuve pénale : un concept de Protée, *Dalloz Actualités*, 17 novembre 2017.

[256] P. Bouzat, *La loyauté dans la recherche des preuves, in* Mélanges L. Hugueney. Problèmes contemporains de procédure pénale, Sirey, 1964, p. 172.

[257] G. Lardeux, *Preuve : règles de preuve – les principes fondamentaux*, Répertoire de droit civil, octobre 2018, points 39 et 380. J. Van Compernolle, *Quelques réflexions sur un principe émergent : la loyauté procédurale, in* Mélanges Guinchard, Dalloz, 2010, p. 413.

[258] A. Leborgne, L'impact *de la loyauté sur la manifestation de la vérité ou le double visage d'un grand principe*, RTD civ. 1996. 535. Y. Perrocheau, Les fluctuations du principe de loyauté dans la recherche des preuves, *LPA*, 2002, no 99, p. 6.

La Cour de cassation a dégagé ce principe dans différents arrêts en rejetant la preuve obtenue de manière déloyale[259]. Néanmoins, cette notion est absente du code de procédure civile[260] ou du code de procédure pénale.

77. Le principe de loyauté dans le droit des données – L'article 5 de la loi informatique et libertés pose les conditions de licéité d'un traitement de données à caractère personnel en définissant les situations justifiant la mise en œuvre du traitement de données. Concernant le traitement des données à caractère personnel, la notion de loyauté se retrouve dans le règlement européen sur la protection des données qui dispose que *« les données à caractère personnel doivent être traitées de manière licite, loyale et transparente »*[261]. Ces dispositions sont reprises dans la loi informatique et libertés qui précise de la même manière que le traitement doit être loyal sans préciser davantage les contours de la notion[262]. Le règlement général sur la protection des données précise que « le fait que des données à caractère personnel concernant des personnes physiques sont collectées, utilisées, consultées ou traitées d'une autre manière et la mesure dans laquelle ces données sont ou seront traitées devraient être transparents à l'égard des personnes physiques concernées »[263], et que « le principe de traitement loyal et transparent exige que la personne concernée soit informée de l'existence de l'opération de traitement et de ses finalités »[264]. Si en droit interne la licéité s'entend de la réunion des principes de légalité et de loyauté, le droit européen semble opérer une distinction entre licéité et loyauté, visant les deux. La loyauté semble alors renvoyer aux obligations qui incombent au responsable du traitement telles que l'information des personnes concernées, l'effectivité des garanties comme le droit d'accès ou la sécurité des données.
Il convient de s'intéresser au principe de loyauté dans la collecte de preuves (§1.) pour observer son application dans la collecte de données à caractère personnel (§2.).

[259] Cass. AP, 7 janvier 2011, *pourvoi* n°09-14.667.
[260] Tout au plus, l'article 763 du code de procédure civile dispose que le juge veille *« au déroulement loyal de la procédure »*.
[261] Art. 5 1. a) du règlement général sur la protection des données.
[262] Art. 4 de la loi informatique et libertés. On retrouve des dispositions similaires au point 26 de la directive UE 2016/680 dite directive police justice.
[263] Considérant 39 du règlement général sur la protection des données.
[264] Considérant 60 du règlement général sur la protection des données.

§1. Le principe de loyauté dans la collecte de preuves

78. La loyauté – L'application du principe de loyauté dans la collecte de preuve renvoie à l'idée de déontologie et à celle d'un comportement ou d'une morale[265]. L'absence de définition dans les textes et la jurisprudence fluctuante amènent à s'interroger sur la portée ambivalente du principe (A.) qui de plus est distincte en fonction de la nature du contentieux (B.).

A. Portée ambivalente du principe de loyauté de la preuve

79. Principe ambivalent – L'ambivalence qui entoure le principe de loyauté de la preuve est la conséquence de plusieurs constats. L'absence de définition du principe (1°) et la construction jurisprudentielle et doctrinale de la loyauté (2°) ont pu créer certaines zones d'ombre.

1° L'absence de définition de la loyauté

80. Absence de définition textuelle – Le premier constat que l'on peut faire s'agissant du principe de loyauté de la preuve est son absence de définition dans les textes. Le terme de loyauté renvoie aux notions d'honneur, probité et droiture. L'absence de définition de la notion de loyauté et son application aux côtés du principe de licéité de la preuve conduisent à une confusion certaine des deux notions.
Les propositions ou projets de définitions ont toujours été abandonnés ou rejetés laissant au juge le soin de fixer les contours du principe, comme par exemple lors des travaux préparatoires de la loi du 15 juin 2000 qui suggéraient d'inscrire le principe dans l'article préliminaire du code de procédure pénale.

81. La question de la reconnaissance du principe de loyauté en droit interne – Dans un rapport[266] remis à la garde des sceaux en janvier 2018, la question a été soulevée d'inscrire la loyauté dans les principes directeurs du procès au sein du code de procédure civile. Cette proposition n'a toutefois pas été suivie d'effets. Apportant son avis sur l'arrêt du 7 janvier

[265] L. Belfanti, *Juge d'instruction*, Répertoire de droit pénal et de procédure pénale, Dalloz, octobre 2015.
[266] F. Agostini, N. Molfessis, Rapport, *Amélioration et simplification de la procédure civile*, Chantiers de la justice, référents, janvier 2018, proposition 23, p. 30 et s.

2011[267], Madame Petit, premier avocat général à la Cour de cassation a posé la question de la réelle existence d'un principe de loyauté de la preuve en droit interne. En l'espèce le litige portait sur un contentieux en droit de la concurrence et soulevait la question de l'admissibilité d'enregistrements réalisés à l'insu de la personne concernée et versés au débat comme moyen de preuve. Citant les travaux de Mme Boursier dans sa thèse relative au principe de loyauté en droit processuel[268], elle rappelle le caractère « polymorphe » de la notion de loyauté. Il ressort en effet des nombreux arrêts qui abordent la question de la loyauté de la preuve, ce caractère et ces contours fluctuants qui dépendent beaucoup du domaine et de la nature du litige.

2° Une construction jurisprudentielle et doctrinale d'un principe ambivalent

82. Le caractère fluctuant du principe de loyauté dans la jurisprudence – Le principe de loyauté dans le recueil de preuve est le fruit d'une lente construction jurisprudentielle parfois ambivalente. L'approche du principe de loyauté de la preuve tant dans la doctrine que dans la jurisprudence peut installer un doute quant à ses sources et sa portée. Sans revenir en détails sur ce débat, on peut rappeler que la loyauté a pu être rattachée aux droits de la défense. En ce sens, une partie de la doctrine a vu en la loyauté une composante des droits de la défense, et plus encore, la Cour européenne des droits de l'Homme l'a rattaché au caractère équitable du procès[269].

83. La loyauté comme principe directeur – On retiendra donc l'analyse selon laquelle la loyauté et plus précisément la loyauté de la preuve renvoie à un principe directeur du procès[270].

La Cour européenne des droits de l'homme a rappelé qu'il appartient aux Etats de légiférer en matière de loyauté de la preuve. Néanmoins, elle a admis le recours à une preuve illicite dans le procès à la condition que cette dernière ait été soumise au contradictoire. La Cour européenne considère ainsi que la procédure a respecté les droits de la défense[271].

---

[267] Cass. AP., 7 janvier 2011, *pourvois* n°09-14.316 et 09-14.667. G. Lardeux, Preuve d'une fraude à l'assurance et respect de la vie privée, *Dalloz*, 2014, p.856.

[268] M.E. Boursier, *Le principe de loyauté en droit processuel*, Dalloz 2003, Thèse.

[269] Notamment dans un arrêt du 25 juin 2015. Cour E.D.H., 25 juin 2015, 22037/13, *Christian Canonne c/ France*. Voir sur le sujet et les différentes approches, S. Guinchard, C. Chanais, C. S. Delicostopoulos, L. S. Delicostopoulos, M. Douchy-Oudot, F. Ferrand, . Lagarde, V. Magnier, H. Ruiz Fabri, L. Sinopoli, J-M. Sorel, *Droit processuel. Droits fondamentaux du procès*, 10 ed, Précis, Dalloz, Paris, 2019, p.1326 ets.

[270] J. Carbonnier, *Droit civil, Introduction*, 27e ed. Thémis, PUF, 2002.

[271] Cour EDH, 12 juillet 1988, *Schenk c/ Suisse*, requête n° 10862/84. A noter néanmoins que dans l'arrêt *Texeiro de castro contre Portugal* du 24 juin 1996, La Cour EDH s'est montrée plus restrictive rejetant la preuve

L'étude de la jurisprudence de la Cour de cassation permet d'observer le caractère fluctuant attaché à la notion de loyauté et ce même lorsqu'elle est appliquée à la recherche et au recueil de preuves[272]. Ainsi pour faire un très bref résumé, on s'aperçoit que l'application qui en est faite varie en fonction du type, de contentieux. La loyauté semble alors « présumée »[273] en matière de recueil de preuves de la faute dans une procédure de divorce. La Cour de cassation se montre plus « pragmatique »[274] en matière commerciale et beaucoup plus en matière pénale s'agissant des preuves collectées et rapportées par les particuliers[275], le principe ne s'appliquant alors pas.

B. Une application distincte du principe de loyauté en fonction du contentieux

84. Une application distincte en droit civil et pénal – L'application faite du principe de loyauté en matière civile et pénale conduit à envisager distinctement les deux matières. La non application de l'exigence de loyauté aux parties privées en matière pénale constitue une différence majeure dans la portée du principe. Il convient de s'intéresser successivement à l'application du principe de loyauté dans la collecte des données probatoires en matière civile (1°.) puis pénale (2°.).

1° L'application du principe de loyauté en matière civile

85. La déloyauté de la collecte de données probatoires par l'usage de stratagèmes – La Cour de cassation a pu juger irrecevable les preuves collectées par le recours à un stratagème en matière sociale par exemple[276]. En l'espèce, l'employeur avait diligenté de faux clients afin de surveiller un salarié. La notion de stratagème en matière civile reste toutefois source d'incertitudes[277]. La question a pu se poser s'agissant de données collectées sur les comptes privés de réseaux sociaux.

La Cour de cassation vient d'apporter des précisions dans un arrêt récent en date du 30 septembre 2020 dans un litige opposant un employeur et son salarié licencié disciplinairement

illicite. En l'espèce, l'utilisation de cette preuve obtenue illicitement avait été déterminante dans le prononcé de la condamnation.

[272] Voir sur la question, A. Bergeaud-Wetterwald, Du bon usage du principe de loyauté des preuves ?, *Droit pénal*, n°4, avril 2014, étude7.

[273] Avis de Mme Petit, premier avocat général, sous arrêts du 7 janvier 2001 *pourvois* n° 09-14.316 et 09-14.667.

[274] *Ibid*.

[275] Cass. AP, 10 novembre 2017, *pourvoi* n° 17-82.028.

[276] Cass., soc., 19 novembre 2014, *pourvoi* n° 13-18.749.

[277] G. Lardeux, *Preuve*, Répertoire de droit civil, *op. cit.*.

sur le fondement de données collectées sur son compte privé « *Facebook* ». La Cour de cassation a écarté l'existence de tout stratagème mis en œuvre par l'employeur puisque les données en question lui avaient été transmises spontanément par un tiers qui y avait accès. De fait, la Cour de cassation n'a pas retenu le caractère déloyal du recueil de preuves[278]. Pour autant, s'il n'est pas déloyal, le procédé ne doit pas non plus porter atteinte à la vie privée. La Cour de cassation rappelle ainsi la nécessité de mettre en balance tous les intérêts en présence précisant que l'employeur peut produire à titre de preuve des données collectées sur un compte « *Facebook* » et transmises par un autre salarié, dans le cadre de l'exercice du droit à la preuve. En l'espèce, la collecte des données était proportionnée au but poursuivi, en l'espèce pour l'employeur la confidentialité de ses affaires[279].

2° L'application du principe de loyauté en matière pénale

86. Champ d'application – Il est depuis longtemps admis qu'en matière pénale la loyauté tend à s'appliquer aux preuves recueillies par les autorités publiques, la jurisprudence permettant aux parties privées de faire usage de preuves obtenues de manière déloyale[280].
La Cour de cassation a rappelé ce principe récemment dans un arrêt du 1er décembre 2020. Ainsi rappelant que le principe de loyauté et de légalité tendent à ne s'appliquer qu'aux autorités, elle a considéré que le versement au dossier de données probatoires remises aux autorités par un organe de presse ne peut être considéré comme déloyal du fait de l'ignorance des procédés de recueil utilisés[281].

87. La loyauté dans la collecte probatoire, une notion aux contours flous – Consacrée par la jurisprudence et la doctrine, la loyauté souffre d'une absence de définition stricte qui en fait un principe aux contours flous empreint d'incertitudes. Cette absence de définition a certainement contribué à instaurer une certaine confusion en la matière amenant parfois à un rapprochement entre la notion de loyauté et celle de légalité matérielle. Parfois attachée à l'idée d'une faute ou d'une provocation à l'infraction parfois à la simple complicité indirecte, la jurisprudence semble encline à apporter des éléments permettant de cerner un peu plus les contours de la loyauté et confirmant l'idée née dans la doctrine d'une autonomie du principe.

[278] Cass., soc., 30 septembre 2020, *pourvoi* n° 19-12.058. C. Lhomond, Droit à la preuve de l'employeur, loyauté de la preuve et respect de la vie privée « numérique » des salariés une nouvelle articulation, *Revue droit du travail*, 2020, p. 764.
[279] G. Loiseau, La preuve par Facebook, *JCP G*, 2 novembre 2020, 1226.
[280] Cass., crim., 27 novembre 2013, *pourvoi* n°13-85.042, Jurisdata n°2013-026728.
[281] Cass., crim., 1er décembre 2020, *pourvoi* n° 20-82.078.

88. La preuve déloyale pour contribution des autorités à la collecte – Dans un arrêt du 20 septembre 2016, la Cour de cassation est venue apporter des précisions sur l'application faite du principe de loyauté aux seules autorités considérant que la simple participation de celles-ci à la collecte de données probatoires présentées par une partie suffit à caractériser la déloyauté. En l'espèce, un requérant présentait comme preuve un enregistrement effectué à l'insu d'un individu. L'implication des autorités dans la collecte de la preuve l'a entachée de déloyauté[282]. Finalement, semble frappée de déloyauté la preuve rapportée par un particulier si les autorités sont impliquées dans sa collecte.

Néanmoins, l'Assemblée plénière a estimé que cette participation directe ou non ne pouvait être déduite de simples constatations et donc que le procédé n'était pas déloyal, laissant supposer la nécessité d'un rôle actif des autorités pour caractériser la déloyauté[283].

89. Le recours aux stratagèmes – Initialement la jurisprudence déduisait la déloyauté de l'existence d'une provocation à l'infraction. La distinction entre provocation à la preuve et provocation à l'infraction repose sur l'implication active ou non de l'autorité judiciaire. Si cette notion a été précisée par la jurisprudence, la doctrine reste partagée concernant la frontière entre les deux procédés. Dans un arrêt du 30 avril 2014[284], la chambre criminelle de la Cour de cassation a jugé loyal le procédé mis en œuvre par les autorités judiciaires visant la création d'un site internet relatif à la fraude à la carte bancaire, leur permettant ainsi d'identifier les auteurs de telles infractions. La Cour de cassation n'a pas estimé que ce procédé incitait à la commission de fraudes. La Cour de cassation a rappelé ce principe que la preuve ait été recueillie par les autorités françaises ou étrangères[285]. Aussi, dans un arrêt du 7 janvier 2014[286], la Cour de cassation a jugé déloyal et contraire aux droits de la défense le procédé visant à sonoriser la cellule d'un gardé à vue, cette dernière étant placée à côté de celle d'un complice présumé et permettant ainsi de recueillir leur conversation[287].

---

[282] Cass., crim., 20 septembre 2016, *pourvoi* n° 16-80.820. Affaire dite « Roi du Maroc ».
[283] Cass., AP, 10 novembre 2017, *pourvoi* n° 17-82.028. Affaire dite « Roi du Maroc ».
[284] Cass., crim., 30 avril 2014, *pourvoi* n° 13-88.162.
[285] De la même manière, dans l'arrêt du 6 février 2007, la Cour de cassation a jugé déloyal le procédé visant la création par les autorités étrangères d'un site pédopornographique permettant d'appréhender un suspect. En effet, suite aux informations recueillies et transmises aux autorités françaises, l'individu avait été poursuivi. Par cet arrêt, la Cour de cassation réaffirme l'obligation de loyauté dans le recueil de la preuve par les autorités françaises ou étrangères.
[286] Cass. crim., 7 janvier 2014, *pourvoi* n°13-85.246.
[287] Voir par exemple, J.F. Renucci, Loyauté des preuves et distinction entre « provocation à l'infraction » et « provocation à la preuve », *RSC*, 2014, p.843. L'auteur s'appuie sur les deux arrêts pour illustrer « les nouvelles frontières » entre les deux notions.

90. La définition des contours de la déloyauté – C'est précisément par l'arrêt du 7 janvier 2014 que la Cour de cassation est venue apporter des précisions sur les contours de la notion de « déloyauté ». La chambre criminelle de la Cour de cassation a cassé une décision prise sur le fondement de preuves obtenues par le recours au procédé de sonorisation de cellules. En l'espèce, différents suspects avaient été placés en garde à vue dans des cellules contigües et sur instruction du juge, les cellules avaient été sonorisées. La Cour de cassation a considéré que le procédé était déloyal, non pas du fait de la sonorisation des cellules, mais du fait que le procédé avait été mis en œuvre dans le but précis que les individus s'auto-incriminent. La Cour de cassation ne rejette donc pas le recours à la sonorisation mais le procédé global mis en œuvre[288]. La Cour de cassation confirme donc ici l'autonomisation du critère de loyauté dans l'administration de la preuve et rappelle l'interdiction générale du recours aux stratagèmes[289]. Cet arrêt marque la réelle autonomie de la loyauté par rapport à la légalité puisque la Cour de cassation dénonce un procédé qui, s'il n'est pas contraire aux exigences légales, apparait globalement déloyal[290].

Cette interprétation a été confirmée par l'Assemblée plénière dans un arrêt du 6 mars 2015[291]. Finalement, la déloyauté semble attachée à une certaine intention dans le contournement de la loi[292].

Partant de cette esquisse de définition de la loyauté par ce qu'elle n'est pas, il convient de s'intéresser à l'application qui en est faite au regard de certains procédés de collecte.

§2. L'application du principe de loyauté dans la collecte de données à caractère personnel

91. Le principe de loyauté dans la collecte de données à caractère personnel – Il est évident que le recueil de preuves entraine la collecte de données à caractère personnel. Le règlement général sur la protection des données et la loi informatique et libertés incluent la collecte de données dans la notion générale de traitement qu'ils encadrent. L'intérêt du sujet est d'aborder la question de cette collecte et de l'exigence de loyauté au regard du caractère

[288] J. Danet, Principe de loyauté des preuves et sonorisation des cellules de garde à vue, *RSC*, 2014, 130.
[289] A. Bergeaud-Wetterwald, Preuve. Du bon usage du principe de loyauté des preuves ? (A propos de l'arrêt rendu par la chambre criminelle de la Cour de cassation le 7 janvier 2014), *Droit pénal*, n°4, avril 2014, étude 7.
[290] O. Decima, De la loyauté de la preuve pénale et de ses composantes, *op. cit.*
[291] Cass., AP, 6 mars 2015, *pourvoi* n°14-84.339. C. Girault, Quand la loyauté dicte sa loi, *AJ Pénal*, 2015, p. 362.
[292] On retrouve cette idée de critère intentionnel dans l'arrêt du 31 mars 2015 (n° 14-86.913). La chambre criminelle de la Cour de cassation n'a pas retenu la déloyauté de la preuve. En l'espèce un individu placé en garde à vue avait délivré des données importantes à un officier de police lors de la pause avant son audition formelle. Ces données probatoires avaient été versées au dossier. La Cour de cassation a considéré qu'il n'y avait pas de la part de l'officier une intention de faire parler l'individu dans le but qu'il s'auto-incrimine.

personnel des données. Il convient de s'intéresser à la collecte loyale de données à caractère personnel en matière civile (A.), puis en matière pénale (B).

A. La collecte loyale de données à caractère personnel en matière civile

92. La loyauté dans les nouveaux modes de collecte probatoire – La question de la loyauté dans la collecte de données à caractère personnel en matière civile, s'apprécie au regard de la nature des données. Le sujet amène à s'interroger en particulier sur la loyauté dans la collecte de données informatiques (1°) et sur celle résultant de l'usage de dispositifs de surveillance (2°).

1° La loyauté dans la collecte de données informatiques

93. La collecte probatoire sur les réseaux sociaux – Avec le développement des réseaux sociaux, s'est rapidement posé la question de la collecte de données par ce biais. En procédure civile, la question de la loyauté dans la collecte de preuves a trouvé à se poser notamment en matière sociale soulevant des interrogations sur le fait de savoir si l'employeur est en mesure d'user de données issues d'un réseau social comme données probatoires dans un litige l'opposant à un salarié.

La première pierre à cet édifice jurisprudentiel a été pour la Cour de cassation de considérer qu'une conversation faite sur un groupe fermé sur *Facebook* constitue une conversation privée qui sur le fondement de la liberté d'expression ne peut être utilisée au fondement d'une procédure de licenciement pour faute[293]. La Cour de cassation opère ainsi une distinction entre conversation « privée » et conversation « publique » sur le réseau social.

Dans un arrêt du 20 décembre 2017, la Cour de cassation a considéré que le fait pour l'employeur d'accéder aux données du compte *Facebook* d'un salarié par le biais du téléphone portable d'un autre constitue un procédé déloyal[294]. La Cour de cassation vise alors un procédé qui porte une « atteinte disproportionnée et déloyale à la vie privée du salarié »[295].

[293] Cass., soc., 12 septembre 2018, *pourvoi* n° 16-11.690.
[294] Cass., soc., 20 décembre 2017, *pourvoi* n° 16-19.609. C. Golhen, *Facebook* : droit au respect de la vie privée VS droit à la preuve, *Dalloz*, 2020, 2383.
[295] *Ibid.*

Néanmoins dans l'arrêt précité du 30 septembre 2020[296], La Cour de cassation n'a pas retenu la déloyauté de la preuve produite par l'employeur à partir de données collectées sur le compte « *Facebook* » d'un salarié. Il faut toutefois noter que la Cour de cassation écarte le recours à tout stratagème du fait que les données avaient été transmises par un autre salarié qui avait lui accès au compte en question. En cela, les juges ont considéré qu'il n'y avait pas eu de manœuvre déloyale.

2° La loyauté dans la collecte de données par l'usage de dispositifs de surveillance

94. La loyauté dans la surveillance des salariés – La reconnaissance prétorienne du principe de loyauté probatoire s'est faite en matière de droit du travail s'agissant de données captées à l'insu des salariés[297]. Ainsi, tout système visant la captation de sons ou d'images des salariés ne peut être licite et loyal que si ces derniers ont été préalablement informés de l'existence du dispositif[298]. La déloyauté est alors attachée au critère de clandestinité.

95. Les enregistrements clandestins – La question est de savoir s'il est possible de procéder, à son insu, à l'enregistrement des propos d'une personne (conversation téléphonique par exemple) et de produire cet enregistrement comme preuve dans une procédure. La question s'est posée dans un arrêt du 7 octobre 2004[299] en matière de succession. La Cour de cassation se fondant sur l'article 9 du code de procédure civile[300] et sur l'article 6 de la Convention européenne des droits de l'Homme, estime qu'un tel enregistrement est déloyal et rend irrecevable sa production en justice. Là encore la matière pénale est plus permissive puisqu'il est admis de longue date la production d'enregistrements parfois même issus d'appels téléphoniques anonymes effectués par la victime elle même[301]. La jurisprudence semble donc rejeter tout enregistrement qui serait fait à l'insu de la personne concernée en matière civile au nom du principe de loyauté de la preuve. De manière générale, tout enregistrement clandestin est empreint, en matière civile, de déloyauté[302].

[296] Cass., soc., 30 septembre 2020, *pourvoi* n° 19-12.058. C. Lhomond, Droit à la preuve de l'employeur, loyauté de la preuve et respect de la vie privée « numérique » des salariés une nouvelle articulation, *Rev. trav.*, p. 764.
[297] Cass., soc., 20 novembre 1991, *pourvoi* n° 88-43.120.
[298] Cass., civ., 2 février 2011, *pourvoi* n° 10-14.263.
[299] Cass. civ. 2e, 7 octobre 2004, *pourvoi* n°03-12.653.
[300] Art. 9 du code de procédure civile *« Il incombe à chaque partie de prouver conformément à la loi les faits nécessaires au succès de sa prétention ».*
[301] Cass. crim., 25 janvier 1994, *pourvoi* n°9381.041.
[302] Par exemple en matière commerciale, Cass., com., 25 février 2003, *pourvoi* n° 01-02.913.

96. La géolocalisation – En droit civil de la preuve, la collecte de données probatoire par le biais de dispositif de géolocalisation trouve à se poser notamment en droit social. Le recours à de tels moyens de surveillance a soulevé des interrogations en termes de légalité mais aussi pose la question de la loyauté. Dans un arrêt du 3 novembre 2011, la chambre sociale de la Cour de cassation a considéré que la mise en place d'un système de géolocalisation des salariés dans une entreprise dans le but de contrôler les horaires de travail s'agissant d'un salarié libre d'organiser son temps de travail est illicite[303]. La Cour de cassation ne vise en l'espèce pas directement le principe de loyauté mais plutôt celui de licéité. Elle condamne néanmoins le contournement de la loi par l'employeur qui déclare la mise en œuvre d'un système de géolocalisation dans un but permis par la loi pour en faire une application différente.

La question de la loyauté dans la collecte de preuves se pose de manière substantiellement différente en matière pénale.

B. La collecte loyale de données à caractère personnel en matière pénale

97. La loyauté face aux procédés coercitifs – La matière pénale offre beaucoup d'exemples de procédés qui par un usage détourné peuvent caractériser une pratique déloyale. L'étude du traitement des données de par leur caractère personnel invite à s'interroger sur la collecte de certaines données particulières au vu du principe de loyauté de la preuve. Ainsi, il convient de s'interroger sur la loyauté dans la collecte de données informatiques (1°) et sur la loyauté dans la collecte de données de localisation en temps réel (2°)

1° La loyauté dans la collecte de données informatiques

98. La nécessaire adaptation des moyens de recueil – Le développement d'internet et du *big data* ont contribué à multiplier les échanges de données par le biais de l'informatique. A la fois source de nouvelles formes de délinquance et de criminalité, internet a conduit à développer de nouvelles formes d'enquête et de collecte de preuves. Face à la nécessité d'adapter les moyens d'actions et de lutte contre les infractions, de nouveaux procédés de collecte ont été créés qui soulèvent des interrogations en termes de loyauté.

[303] Cass., soc., 3 novembre 2011, *pourvoi* n°10-18.036.

99. Les enquêtes sur internet – De nouveaux moyens de collecte de preuves ont été créés par le législateur qui en application du principe de légalité est venu définir les modalités de leur mise en œuvre[304]. Certains de ces procédés ont pu soulever des interrogations en termes de loyauté dans la collecte de données probatoires.

Par exemple, s'agissant des enquêtes sur internet, la Cour de cassation a eu à se prononcer sur la question de la loyauté en matière de provocation policière sur internet. Reprenant ainsi le principe existant dans une enquête classique, la Cour de cassation a rappelé que toute provocation à la commission d'une infraction par les autorités entache la preuve de déloyauté[305]. En l'espèce, il s'agissait de la mise à disposition d'un site à caractère pédopornographique. La Cour de cassation a considéré que par ce procédé, les autorités incitaient à la commission de l'infraction. Par opposition, la Cour de cassation a considéré que la création par les autorités d'un site internet permettant l'échange entre internautes sur les pratiques à la fraude bancaire, n'était pas contraire au principe de loyauté puisque le procédé ne tend pas à provoquer la commission de l'infraction mais juste à collecter les preuves[306].

100. Les enquêtes sur internet sous pseudonyme – La procédure d'enquête sous pseudonyme a été étendue par la loi du 23 mars 2019[307]. L'article 230-46 du code de procédure pénale prévoie la possibilité pour les autorités d'enquêter pour les crimes et délits commis sur internet et punis d'une peine d'emprisonnement et lorsque cela est nécessaire en utilisant un pseudonyme. Ils peuvent ainsi participer à des échanges y compris avec les suspects et collecter par ce biais toutes données probatoires. Les dispositions de l'article 230-46 du code de procédure pénale visent la constatation des crimes et délits et précisent que le dispositif ne peut avoir pour conséquence d'inciter à la commission d'une infraction.

Le recours à ce dispositif soulève évidement la question de la loyauté sous fond d'éventuelles provocations à l'infraction. Le législateur a toutefois fait le choix d'inscrire dans les dispositions légales l'interdiction d'un usage qui provoquerait l'infraction. On peut donc imaginer qu'une demande d'annulation d'actes relative au recueil de données effectué sous pseudonyme pourrait être présentée au visa du principe de légalité et de loyauté.

---

[304] V. *supra* n°29 s.

[305] Cass., crim., 7 février 2007, *pourvoi* n° 06-87.753.

[306] Cass., crim., 30 avril 2014, *pourvoi* n° 13-88.162. J. Buisson, *Preuve*, Répertoire de droit pénal et de procédure pénale, *op. cit.*

[307] Loi 2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice.

2° La loyauté dans la captation de données en temps réel

101. Développement de nouveaux modes de captation en temps réel – Le développement des moyens de traçage et de géolocalisation ont soulevé des interrogations en termes de licéité de la preuve. Ces procédés en ce qu'ils sont intrusifs dans la vie privée, ont été source de litiges sur le terrain de la légalité imposant au législateur d'intervenir afin de créer une base légale à ces procédés. La question de la loyauté dans la collecte de preuve peut également se poser s'agissant de la mise en œuvre des nouvelles techniques de captation en temps réel (géolocalisation, IMSI-catcher), dans le détournement des dispositions légales qui pourraient être faites. La « volatilité » d'internet a de fait « bousculé » le principe de loyauté de la preuve[308]. Les spécificités de la recherche de preuves sur internet ont conduit le législateur à prévoir des procédés par principe plus intrusifs[309] rendant légal l'usage de stratagèmes sans que ceux-ci ne puissent être frappés de déloyauté[310].

Après une approche basée sur les principes encadrant la licéité de la preuve et de la collecte de données probatoires il peut être intéressant d'observer les règles encadrant le recueil de preuves au regard de la nature de celles-ci rejoignant ici l'approche adoptée en matière de traitement de données personnelles. En effet, le règlement général sur la protection des données et la loi informatique et libertés assurent une protection particulière s'agissant de certaines catégories de données personnelles, notamment lorsqu'il s'agit de traiter des données sensibles. Il s'agit donc de s'intéresser à l'impact de la nature des données sur leur fonction en tant que preuve tant dans leur collecte que dans appréciation.

[308] M.Quéméner, La preuve numérique dans un cadre pénal, *Jurisclasseur communication*, n° 1105 avril 2019. M. Quéméner, La preuve numérique pénale à l'épreuve de la déloyauté, *Actualités du droit, Lamyline*, 27 août 2019.
[309] V. *supra* n°23 s.
[310] M. Quéméner, La preuve numérique pénale à l'épreuve de la déloyauté, *op. cit*.

CHAPITRE 2 : L'IMPACT DE LA NATURE PARTICULIERE DES DONNEES A CARACTERE PERSONNEL SUR LEUR FONCTION PROBATOIRE

102. La collecte de données au vu de leur nature – L'appréhension des questions attachées à la preuve sous l'angle de la nature des données permet d'adopter un raisonnement basé sur l'approche du traitement de données tel que défini par les textes. La loi informatique et libertés et les textes supra nationaux qu'elle transpose définissent des obligations et des interdictions s'agissant du traitement de certaines données. Si, par exemple, la loi informatique et libertés et le règlement général sur la protection des données posent l'interdiction du traitement des données sensibles, l'exercice d'un droit en justice constitue une exception à cette prohibition. Néanmoins, l'analyse de la question de la collecte de preuves sous l'angle des particularités attachées à certains types de données permet un parallèle intéressant avec le sujet.

103. Intérêt du sujet – Il s'agit donc de s'intéresser plus particulièrement aux procédés de collecte de données à vocation probatoire et aux spécificités attachées à la nature des données. Ces dernières peuvent être couvertes par un secret soulevant alors la question de l'accès aux données médicales, bancaires ou détenues par un avocat par exemple. Le sujet soulève également la question de la collecte de données couvertes par le secret des affaires. Découle de ce raisonnement l'analyse de la force probante de ces données. *A priori*, l'étude des principes encadrant l'appréciation de la preuve n'apparait pas utile au vu du sujet, néanmoins, la nature des données à caractère personnel collectées comme preuves dans le procès amène à s'interroger sur la valeur probante de certaines d'entre elles malgré le principe de libre appréciation.

Il convient donc de s'intéresser à la collecte de données à caractère personnel au regard de leur nature (Sect.1) puis de s'interroger sur l'appréciation de ces preuves au regard de la nature des données collectées (Sect.2).

Section 1 : La collecte de données à caractère personnel au regard de leur nature

104. Nature des preuves – Après avoir observé la collecte de données probatoires au regard des principes encadrant la licéité de la preuve, il peut être opportun d'adopter un regard plus particulier, fondé sur la nature des données collectées. Les données collectées dans les procédures en tant que potentielles preuves constituent pour la majorité des données identifiantes. Certaines de ces données à vocation probatoire sont des données relevant dans les textes de dispositions particulières au regard de leur nature. C'est notamment le cas des données protégées par un secret professionnel ou des données scientifiques et médicales qui constituent des données sensibles au sens de la loi. L'approche du sujet en fonction de la nature des données collectées permet de s'interroger à la fois sur le recueil de données protégées et sur la question de l'accès à celles-ci mais soulève aussi la question de la collecte de données dématérialisées.
La recherche de preuves amène à la collecte de données à caractère personnel soumises au secret (§1.). Aussi, à l'ère de la numérisation des échanges et de la communication, la question se pose de la collecte des données numériques (2.).

§1. La collecte de données à caractère personnel soumises au secret

105. Collecte de données protégées – La question qui se pose est celle de la collecte de données protégées en vue de leur production comme preuves. Il s'agit donc ici de s'intéresser aux procédés visant la collecte de données soumises au secret professionnel (A.) puis à celle relevant du secret des sources journalistiques (B.).

A. La collecte de données soumises au secret professionnel

106. Accès aux données couvertes par un secret – Dans leurs prérogatives de recueil de données à vocation probatoire, les autorités judiciaires se trouvent nécessairement confrontées aux données protégées par un secret professionnel. Certaines dispositions viennent faciliter l'accès à ces données.

107. Portée du secret professionnel – Hors les cas où la loi l'autorise, la révélation d'un secret dont on est dépositaire constitue un délit puni par le code pénal[311]. On retrouve des dispositions relatives au secret professionnel dans la grande majorité des codes[312]. Une recherche sur Légifrance permet de faire ressortir plus de 700 résultats relatifs aux dispositions qui encadrent cette notion. La chambre criminelle de la Cour de cassation a précisé que l'obligation de secret qui pèse sur les avocats est générale et absolue[313]. Aussi, le fait d'être tenu au secret et de diffuser cette information à une autre personne elle aussi tenue au secret constitue une violation du secret[314].

La Cour de cassation a eu l'occasion de se prononcer suite à la transmission de plusieurs questions prioritaires de constitutionnalité sur la transmission de données bancaires entre la Commission bancaire et le fonds de garantie[315]. Cette question a permis à la Cour de cassation de préciser que « le principe invoqué de respect du secret professionnel en cours de procès n'est pas un principe ou un droit garanti par la Constitution » ; aussi le secret professionnel ne peut pas venir entraver le droit au procès équitable[316].

---

[311] Art. 226-13 du code pénal « *La révélation d'une information à caractère secret par une personne qui en est dépositaire soit par état ou par profession, soit en raison d'une fonction ou d'une mission temporaire, est punie d'un an d'emprisonnement et de 15 000 € d'amende».*

Art. 226-14 du code pénal *« L'article 226-13 n'est pas applicable dans les cas où la loi impose ou autorise la révélation du secret. En outre, il n'est pas applicable:*

1° A celui qui informe les autorités judiciaires, médicales ou administratives de privations ou de sévices, y compris lorsqu'il s'agit d'atteintes (L. n° 2006-399 du 4 avr. 2006, art. 14) «ou mutilations» sexuelles, dont il a eu connaissance et qui ont été infligées à un mineur ou à une personne qui n'est pas en mesure de se protéger en raison de son âge ou de son incapacité physique ou psychique;

2° Au médecin (L. n° 2015-1402 du 5 nov. 2015, art. 1er) «ou à tout autre professionnel de santé» qui, avec l'accord de la victime, porte à la connaissance du procureur de la République (L. n° 2015-1402 du 5 nov. 2015, art. 1er) «ou de la cellule de recueil, de traitement et d'évaluation des informations préoccupantes relatives aux mineurs en danger ou qui risquent de l'être, mentionnée au deuxième alinéa de l'article L. 226-3 du code de l'action sociale et des familles,» les sévices ou privations qu'il a constatés, sur le plan physique ou psychique, dans l'exercice de sa profession et qui lui permettent de présumer que des violences physiques, sexuelles ou psychiques de toute nature ont été commises. (L. n° 2007-297 du 5 mars 2007, art. 34) «Lorsque la victime est un mineur ou une personne qui n'est pas en mesure de se protéger en raison de son âge ou de son incapacité physique ou psychique, son accord n'est pas nécessaire;»

3° Aux professionnels de la santé ou de l'action sociale qui informent le préfet et, à Paris, le préfet de police du caractère dangereux pour elles-mêmes ou pour autrui des personnes qui les consultent et dont ils savent qu'elles détiennent une arme ou qu'elles ont manifesté leur intention d'en acquérir une. »

[312] Art. L511-33 du code monétaire et financier.

[313] Cass. crim., 7 mars 1989, *pourvoi* n°87-90.500.

[314] Cass. cril. 16 mai 2000, *pourvoi* n°99-85.304.

[315] Il était invoqué la violation par l'article L631-1 III du code monétaire et financier de la Constitution.

[316] Cass. com., 13 avril 2012, *pourvoi* n°12-40.009.

X. Delpech, Pas de QPC sur le fonds de garantie des dépôts bancaires, *Dalloz actualité*, 19 avril 2012.

108. Données protégées et droit à la preuve – La question du secret professionnel trouve nécessairement à se confronter au droit à la preuve. Sur cette question précise la Cour de cassation a jugé que le droit à la preuve ne pouvait faire obstacle à « l'intangibilité » du secret professionnel[317], ce dernier étant « absolu »[318]. La Cour de justice de l'Union européenne semble adopter une conception plus relative du secret professionnel, rappelant la nécessité de concilier les différents intérêts en présence[319]. La jurisprudence interne qui prônait initialement un secret bancaire absolu a néanmoins semblé évoluer au profit d'une reconnaissance d'un droit à la preuve justifiant l'accès et la production des données protégées du fait de leur caractère nécessaire dans l'issue du procès[320]. Aussi, la Cour de cassation admet qu'au titre du respect du contradictoire les données soumises au secret puissent être portées à la connaissance de toutes les parties au procès[321].

Quoi qu'il en soit, les litiges relatifs au secret professionnel sont nombreux et il serait fastidieux de faire une étude globale de la jurisprudence en la matière tant elle est abondante. Si l'on raisonne en termes de données personnelles la question qui se pose est de savoir qu'elle position adopte le législateur et les hautes juridictions concernant le recueil et l'accès aux données à caractère personnel face au secret professionnel.

109. Les perquisitions dans des lieux « protégés » – La question des perquisitions et saisies soulève, s'agissant des données à caractère personnel, celle des perquisitions dans des lieux « protégés » ou tout au moins lieux qui renferment des données protégées. Les perquisitions dans une entreprise de presse, un cabinet d'avocat, de médecin, notaire ou huissier de justice, ne peuvent être décidées et réalisées que par un magistrat, le cas échéant accompagné d'un représentant de l'Ordre de la profession[322]. En toute logique, les données qui seraient collectées de manière irrégulière ne peuvent être versées au dossier d'instruction[323].

---

[317] Cass. civ. 1ère, 4 juin 2014, *pourvoi* n°12-21.244.

[318] G. Lardeux, *Preuve : règles de preuve – les principes fondamentaux*, Répertoire de droit civil, *op. cit.*, points 342. Ce caractère absolu se justifie par un motif d'intérêt général. Il est admis que le secret professionnel quel qu'il soit, garantit l'intérêt général, que ce soit le secret médical, le secret bancaire, le secret de l'avocat…

[319] CJUE, 16 juillet 2015, C-580-13. En l'espèce, une entreprise victime de contrefaçon a demandé à la banque qui a enregistré les transactions litigieuses de fournir les coordonnées de la personne ayant instigué l'opération. La banque a alors refusé au titre du secret bancaire. La rédaction de l'arrêt laisse penser que sa portée dépasse le seul cadre des litiges bancaires.
G. Lardeux, *Preuve : règles de preuve – les principes fondamentaux*, Répertoire de droit civil, Dalloz, *op. cit.*, points 348.

[320] Voir notamment, Cass. com., 15 mai 2019, *pourvoi* n°18-10.491 ; Cass. com., 24 mai 2018, *pourvoi* n°17-27.969. Le raisonnement de la Cour repose sur le caractère nécessaire de la production des documents bancaires.

[321] Cass. crim., 16 février 2010, *pourvoi* n°09-86.363. En l'espèce, un dossier médical avait été versé aux débats.

[322] Art. 56-1 à 56-3 du code de procédure pénale.

[323] Cass., crim., 8 juillet 2020, *pourvoi* n° 19-85.491.

La question plus particulière de la collecte de données détenues par des organes de presse soulève celle du secret des sources.

B. La collecte de données face au secret des sources

110. Consécration du secret des sources journalistiques – Il convient de s'intéresser plus en détails au secret des sources journalistiques qui soulève davantage de questions en termes de levée du secret. Souvent qualifiée de « pierre angulaire de la liberté de la presse »[324], la protection du secret des sources a vu son arsenal juridique se préciser. La loi du 4 janvier 2010[325], bien qu'objet de critiques[326], est venue consacrer plus précisément le droit à la protection du secret des sources journalistiques en intégrant ce dernier dans la loi sur la presse du 29 juillet 1881. Elle modifie ainsi l'article 56-2 du code de procédure pénale et encadre plus strictement les conditions de perquisitions au sein d'entreprises de presse[327]. Par ces nouvelles dispositions, le législateur affirme davantage le droit au secret des sources rendant les données identifiant les sources moins accessibles et plus protégées. La loi de 2010 ne pose pas de définition de ce qu'est le secret des sources ni des sources protégées mais elle dispose qu'il peut être fait exception au principe « *si un impératif prépondérant d'intérêt public le justifie et si les mesures envisagées sont strictement nécessaires et proportionnées au but légitime poursuivi »*[328]. On comprend ici la volonté du législateur de réaffirmer la protection du secret des sources sans pour autant qu'il soit porté atteinte aux droits de la défense et à l'intérêt public[329].

111. Application du secret face à la nécessaire collecte de donnés probatoires – La Cour de cassation a fait application de ces dispositions dans un arrêt du 6 décembre 2011[330]. Elle a alors jugé qu'en permettant à des officiers de police judiciaire d'obtenir les coordonnées

[324] Cour EDH, 27 mars 1996, *Goodwin c/ Royaume-Uni.*
[325] Loi n°2010-1 du 4 janvier 2010 relative à la protection du secret des sources des journalistes.
[326] Voir notamment, A. Chavagnon, La protection des sources journalistiques : la décevante loi n°2010-1 du 4 janvier 2010, *Dalloz*, 2010, p. 275. L'auteure fait référence au manque d'effectivité de la protection des sources journalistiques du fait notamment des pouvoirs d'investigation du juge d'instruction lui permettent de diligenter des perquisitions dans les entreprises de presse ou d'ordonner des écoutes judiciaires.
[327] Ces perquisitions ne peuvent se faire que sur décision écrite et motivée d'un magistrat.
[328] Art. 1er loi 4 janvier 2010, relative à la protection du secret des sources des journalistes.
[329] La Commission nationale consultative des droits de l'homme s'est prononcée sur la réforme du secret des sources proposant notamment que toute levée du secret pour des raisons d'enquête ou d'instruction soit autorisée par le juge des libertés et de la détention. A noter que cette loi a été vivement critiquée notamment par l'absence de sanctions pénales en cas de violation.
[330] Cass. crim., 6 décembre 2011, *pourvoi* n°11-83.970.
S. Lavric, *« Fadettes du monde » : violation du secret des sources*, Dalloz actualité 20 décembre 2011.

téléphoniques de correspondants de journalistes, le droit au secret des sources a été violé. La Cour a estimé que cette mesure était disproportionnée. Finalement, si le législateur a affirmé le droit à la protection du secret des sources des journalistes[331], la Cour de cassation admet qu'il soit procédé à des perquisitions dans les entreprises de presse permettant de recueillir les données concernées[332]. Dans un arrêt du 25 février 2014, la Cour de cassation rappelle qu'une ingérence dans le secret des sources est possible si elle répond à un impératif prépondérant d'intérêt public[333], reprenant ainsi la jurisprudence de la Cour européenne des droits de l'Homme[334]. Ces arrêts permettent de comprendre la position de la Cour de cassation sur la question qui cherche le juste équilibre entre protection du secret et droits de la défense. La question du juste équilibre entre les droits se pose également s'agissant des données soumises au secret médical[335].

Au-delà de la question de l'accès et de la collecte aux données protégées se pose celle de la collecte de données numériques qui trouve de plus en plus à se poser du fait du développement exponentiel d'internet et du phénomène de *big data*. Cette évolution a poussé le législateur à adapter les textes en vigueur dans une société de plus en plus numérique.

§2. La collecte de données à caractère personnel numériques

112. Adaptation des textes à l'informatisation – La dématérialisation des échanges et le développement d'internet soulèvent la question des procédés de collecte de ces données numériques. Aussi, au-delà de la question de la collecte se pose celle de l'accès à des données parfois inaccessibles car verrouillées par divers procédés. Il convient donc de s'interroger en premier lieu sur la création des réquisitions portant sur des données numériques (A.) pour ensuite s'intéresser à la question plus particulière de l'accès aux données chiffrées (B.).

---

[331] Art. 109 al 2 du code de procédure pénale.

[332] Cass. crim., 5 décembre 2000, *pourvoi* n°00-85.695. J. Buisson, *Preuve*, Répertoire de droit pénal et de procédure pénale, *op. cit.*

[333] Cass. crim., 25 février 2014, *pourvoi* n°13-84.761. En l'espèce, la Cour d'appel avait rejeté la requête en annulation des pièces sans démontrer l'existence d'un impératif prépondérant d'intérêt public.
S. Lavric, *Perquisitions au domicile d'un journaliste : atteinte au secret des sources*, Dalloz actualité 5 mars 2014.

[334] Dans l'arrêt Goodwin c/ RU du 27 mars 1996, la Cour E.D.H. fait référence à l'intérêt prépondérant d'ordre public » pour justifier l'atteinte faite à la liberté de la presse lors de perquisitions dans une entreprise de presse. Aussi, dans un arrêt de grande chambre du 14 septembre 2010 (Sanoma Uitgevers B.V. c/ Pays-Bas, req. n°38224/03), la CEDH rappelle que toute atteinte au secret des sources doit être encadrée par des garanties procédurales fonction de « l'importance du principe enjeu ».

[335] La question de l'accès aux données soumises au secret médical sera abordée dans son ensemble en seconde partie.

A. Les réquisitions portant sur des données numériques

113. Nécessaire adaptation des textes au numérique – En matière de réquisition de données informatiques, la loi du 9 mars 2004 dont les dispositions ont été précisées par le décret du 26 octobre 2007[336] est venue créer une procédure de « réquisition électronique » permettant aux autorités chargées de l'enquête de demander la transmission des seules données utiles à l'enquête. La Commission nationale de l'informatique et des libertés a exprimé un avis concernant le projet de décret[337]. Elle a relevé que la transmission par voie électronique des réquisitions permettrait une meilleure célérité. Toutefois, elle rappelle que le procédé vise un grand nombre de données. Néanmoins, des garanties existent puisque seules les données « utiles » à la manifestation de la vérité peuvent être transmises à condition de ne pas être protégées par un secret. De plus, sur autorisation du juge des libertés et de la détention saisi par le procureur de la République, un enquêteur peut requérir tout opérateur de communications électroniques d'assurer la préservation des données numériques d'utilisateurs[338]. En pratique, des réquisitions permettent l'accès aux données numériques, leur copie ou leur saisie quel que soit leur support et y compris aux données chiffrées qui nécessitent un traitement particulier.

B. Le cas particulier de l'accès aux données chiffrées

114. L'accès aux données chiffrées – Dans le cadre d'une procédure, le juge en charge de l'enquête peut requérir toute personne de fournir les codes permettant l'accès à des données numériques si ces dernières sont verrouillées. Cette demande peut être présentée à des tiers. Ce dispositif permet d'accéder à des données protégées[339]. Le Conseil constitutionnel saisi d'une question prioritaire de constitutionnalité, a rappelé que ce dispositif ne pouvait être utilisé que par les autorités judiciaires dans le cadre de recueil de preuves dans une procédure et que le fait de refuser de donner les clés de déchiffrement dans le cadre d'une enquête

[336] Décret n°2007-1538 du 26 octobre 2007 relatif aux demandes de mise à disposition de données par voie électronique et modifiant le code de procédure pénale. Avant le décret, une telle réquisition nécessite la saisie du matériel informatique ou la copie intégrale des disques durs. En cela, la nouvelle procédure a pu être jugée moins intrusive et plus respectueuse des droits.
[337] Délibération CNIL n°2006-152 du 30 mai 2006 portant avis sur un projet de décret relatif aux réquisitions télématiques ou informatiques.
[338] Loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique. Art. 6 I.
[339] M. Quéméner, Le refus de déchiffrement à l'épreuve des droits fondamentaux, *Dalloz IP/IT*, 2018, p. 514.

judiciaire constitue un délit d'entrave à la justice[340]. Le Conseil constitutionnel a, dans sa décision du 30 mars 2018 jugé que ces dispositions ne portent pas atteinte au droit de ne pas s'accuser, au droit au respect de la vie privée ni au secret des correspondances. La loi du 21 juin 2004 pour la confiance dans l'économie numérique a alourdi la peine s'agissant de l'usage de la cryptologie pour commettre un délit ou un crime. Cette loi est venue définir la cryptologie comme « *« tout matériel ou logiciel conçu ou modifié pour transformer des données, qu'il s'agisse d'informations ou de signaux, à l'aide de conventions secrètes ou pour réaliser l'opération inverse avec ou sans convention secrète. Ces moyens de cryptologie ont principalement pour objet de garantir la sécurité du stockage ou de la transmission de données, et permettant d'assurer leur confidentialité, leur authentification ou le contrôle de leur intégrité »*[341].

Face à la multiplication des délits et crimes réalisés au moyen de cryptologie, la pénalisation du refus de mettre à disposition les clés de déchiffrement apparait évidente. Aussi, depuis la loi du 15 novembre 2001 sur la sécurité intérieure, l'article 230-1 du code de procédure pénale prévoit une procédure de mise au clair des données chiffrées. Ainsi, si les données numériques collectées lors d'une enquête ou d'une instruction sont chiffrées ou modifiées par un procédé de cryptologie ou d'authentification, le procureur de la République, le juge d'instruction ou l'officier de police judiciaire sur autorisation de ces derniers, peuvent requérir toute personne physique ou morale en mesure de déchiffrer les données.

Un décret du 24 avril 2017 est venu créer l'agence nationale des techniques d'enquêtes numériques judiciaires compétente en la matière[342].

Quel que soit le procédé de collecte des données se pose la question de l'appréciation de ces données comme preuve dans la procédure. Bien que prédomine le principe de libre appréciation des preuves par le juge, force est de constater que certaines d'entre elles

[340] Cons. Const., 30 mars 2018, n° 2018-696 QPC. La question portait sur la constitutionnalité de l'article 434-15-2 du code pénal. *« Est puni de trois ans d'emprisonnement et de 270 000 € d'amende le fait, pour quiconque ayant connaissance de la convention secrète de déchiffrement d'un moyen de cryptologie susceptible d'avoir été utilisé pour préparer, faciliter ou commettre un crime ou un délit, de refuser de remettre ladite convention aux autorités judiciaires ou de la mettre en oeuvre, sur les réquisitions de ces autorités délivrées en application des titres II et III du livre Ier du code de procédure pénale.*
Si le refus est opposé alors que la remise ou la mise en oeuvre de la convention aurait permis d'éviter la commission d'un crime ou d'un délit ou d'en limiter les effets, la peine est portée à cinq ans d'emprisonnement et à 450 000 € d'amende ».

[341] Loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, art. 29.

[342] Décret n° 2017-614 du 24 avril 2017 portant création d'un service à compétence nationale dénommé « Agence nationale des techniques d'enquêtes numériques judiciaires » et d'un comité d'orientation des techniques d'enquêtes numériques judiciaires.

semblent emporter davantage la conviction. Ce constat soulève en particulier la question de la place de la preuve scientifique dans le procès.

Section 2 : L'impact de la nature des données dans l'appréciation de la preuve

115. Le principe de libre appréciation des preuves – La libre appréciation des preuves se retrouve aux articles 427 du code de procédure pénale. En matière civile, ce principe n'est évoqué qu'à l'article 1381 du code civil s'agissant de témoignages. L'application de ce principe a donc pu être qualifiée de « répandue et diffuse »[343]. La notion même de libre appréciation de la preuve renvoie selon les contentieux à d'autres notions tels que l'intime conviction en procédure pénale, ou « appréciation souveraine de la force probante »[344]. Ainsi, le juge peut écarter des moyens de preuves pour fonder sa décision sur d'autres. Il peut notamment écarter les conclusions d'une expertise. En matière criminelle, l'article 353 du code de procédure pénale illustre cette notion : *« La loi ne demande pas compte aux juges des moyens par lesquels ils se sont convaincus, elle ne leur prescrit pas de règles desquelles ils doivent faire particulièrement dépendre la plénitude et la suffisance d'une preuve ; elle leur prescrit de s'interroger eux-mêmes dans le silence et le recueillement et de chercher, dans la sincérité de leur conscience, quelle impression ont faite, sur leur raison, les preuves rapportées contre l'accusé, et les moyens de sa défense. La loi ne leur fait que cette seule question, qui renferme toute la mesure de leurs devoirs : « Avez-vous une intime conviction ? » ».* De manière générale, l'article 427 du même code dispose que *« Hors les cas où la loi en dispose autrement, les infractions peuvent être établies par tout mode de preuve et le juge décide d'après son intime conviction. Le juge ne peut fonder sa décision que sur des preuves qui lui sont apportées au cours des débats et contradictoirement discutées devant lui ».* On comprend ainsi qu'au vu des éléments en sa possession, le juge doit se forger une conviction qui lui permettra de trancher le litige qui lui est soumis. De cette conviction découlera une « vérité »[345]. La portée du principe d'intime conviction a toujours divisé, certains faisant référence à une « certitude » du juge, d'autres à une « forte probabilité »[346].

[343] E. Vergès, G. Vial, O. Leclerc, *Droit de la preuve, op. cit,* p. 434.
[344] Cass., civ., 3e, 23 mars 2005, *pourvoi* n°03-19.281.
[345] Cette notion a fait l'objet de nombreux débats. Certains distinguant la vérité absolue et la vérité judiciaire. Voir à ce sujet, D. Bauer, La vérité en droit : concepts amis ou ennemis ?, *LPA*, n°044, 1er mars 2019, p. 4.
[346] E. Vergès, La réforme du droit de la preuve civile : enjeux et écueils d'une occasion à ne pas manquer, *Dalloz*, 2014, p. 617.

Comme le suggère l'adage, *in dubio pro reo*, le doute profite à l'accusé. L'intime conviction du juge doit emporter une décision qui ne laisse pas de place au doute[347].

116. Les conflits de preuves – Du principe de libre appréciation des preuves découle l'absence de hiérarchie entre elles. Toutefois, certaines situations imposent de régler des conflits de preuves entre elles. C'est notamment le cas en matière de preuve encadrée par la loi. Une hiérarchie peut être établie en fonction des différentes catégories de preuves. Ainsi, en matière civile, il existe une prédominance de l'écrit sur les autres preuves. L'acte authentique constitue une preuve parfaite jusqu'à inscription de faux. Ainsi, il a une valeur probante supérieure à une preuve imparfaite. Toutefois, face à un aveu judiciaire ou un serment décisoire, l'écrit peut s'effacer au profit de ces derniers. Cela ne signifie toutefois pas que tous les écrits ont la même valeur. Ainsi, l'acte authentique aura toujours plus de valeur que l'acte sous signature privé.

Lorsque plusieurs preuves d'égale valeur probante se retrouvent en concurrence, la loi permet alors au juge d'user de son pouvoir d'appréciation et de déterminer la preuve qui selon lui est la plus convaincante. L'article 1368 du code civil dispose en effet qu'en matière de conflit de preuve littérale, le juge doit par tout moyen déterminer la preuve la plus vraisemblable, peu importe son support.

Enfin, on peut mentionner l'existence d'une égalité entre écrit papier et écrit électronique. Pour rappel, la loi du 13 mars 2000[348] a érigé l'écrit électronique au même niveau que l'écrit papier, lui attribuant ainsi la même valeur probatoire[349]. Il en découle alors qu'en cas de conflit de preuve entre un écrit papier et un écrit électronique, il appartient au juge de déterminer le plus vraisemblable des deux.

117. Valeur probante au regard de la nature des données à caractère personnel – S'agissant des données à caractère personnel intervenant comme preuves dans une procédure,

[347] Ces dispositions se retrouvent à l'article 304 du code de procédure pénale s'agissant des arrêts d'assises. Néanmoins la place du doute dans le procès soulève toujours de vives interrogations. Parallèle de l'intime conviction, le juge a l'obligation de motiver ses décisions. Voir, S. Guinchard, *Procès équitables, garanties procédurales,* Répertoire de procédure civile, Dalloz, mars 2017, 581. La motivation des décisions de justice *« est le rempart contre l'arbitraire en forçant le juge à prendre conscience de son opinion, de sa portée. Elle procure au plaideur une justification de la décision et permet de procéder à une analyse scientifique de la jurisprudence. Enfin, elle permet à la Cour de cassation d'exercer son contrôle ».*

[348] Loi 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique.

[349] Art. 1366 du code civil.
Par exemple, J.D. Pellier, La forme et la force de l'écrit électronique, *Dalloz actualité*, 6 sept. 2018.
Y. Favier, *Correspondances, messages électroniques*, Répertoire de droit civil, Dalloz, octobre 2019, 103.

la question se pose de la valeur probante de celles-ci au vu notamment de leur nature. Les évolutions technologiques et scientifiques ont permis le recours à de nouveaux procédés et à de nouvelles preuves pour lesquelles la question de la force probante a pu se poser remettant parfois en doute le principe d'égalité des preuves entre elles. Sans vouloir faire une analyse exhaustive de ces procédés, il peut être intéressant de soulever ces questions s'agissant des données génétiques et des données numériques. Il s'agit donc de s'intéresser à la valeur probante des données scientifiques (§1.) puis à celle des données numériques (§2.).

§1. La valeur probante des données scientifiques

118. Limitation de la force probante – La loi informatique et libertés dans son article 47 interdit de prendre des décisions impliquant l'appréciation du comportement d'un individu ou qui produit des effets juridiques envers celui-ci sur le fondement de données issues d'un traitement automatisé. Cette prohibition est reprise dans l'article 95 de la loi informatique et libertés s'agissant des dispositions relatives aux traitements de données par les autorités en matière de prévention et lutte contre les infractions. Ces dispositions reprennent celles de l'article 11 de la directive Police-Justice.

Cette interdiction apparait comme une garantie pour les individus d'une justice qui ne serait pas le résultat de systèmes automatisés mais sur laquelle l'être humain conserve un libre arbitre et une liberté d'appréciation. Cela renvoie évidement à la question de la productivité de la justice et aux craintes que celle-ci entraine quant à une déshumanisation possible ou non de la justice. Il s'agit donc de s'interroger sur le passage d'une donnée scientifique à une preuve juridique (A.) et sur les potentielles évolutions quant au recours aux données biométriques dans le procès (B.).

A. De la donnée scientifique à la preuve juridique

119. Terminologie – Pour reprendre les propos du Doyen Carbonnier, *« Prouver le droit, c'est faire admettre au juge sinon comme vrai […] du moins comme probable »*. La preuve juridique et la preuve scientifique ont souvent été opposées dans la doctrine, la science présentée comme plus exacte face aux présomptions du juge[350]. Ainsi, le droit a pu être

[350] Dans ce sens, la preuve juridique a pu être qualifiée « d'évitement de la science […] une vérité fausse ». A.M. Leroyer, *Les fictions juridiques*, Thèse, sous la direction de M. Gobert, Paris 2, 1995.

présenté comme un « modérateur de la vérité »[351] en ce qu'il permet parfois de fonder une vérité juridique alors même que la science ne se positionne pas en ce sens. C'est notamment le cas quand le juge tranche un litige au nom du principe de précaution alors que la science, elle, n'a pas un avis certain sur la question ou ne se prononce pas[352], ou lorsque le juge prend sa décision sur le fondement de présomptions[353]. Néanmoins, les évolutions de la science ont marqué le droit de la preuve notamment par la révolution de l'expertise ADN et ont tendu à donner plus d'importance à la preuve scientifique dans le procès. On ne peut donc nier l'importance relative qu'a pris la science dans le procès et notamment celle de la donnée biométrique en tant que preuve. La biométrie renvoie à l'identification des individus par l'étude de leurs caractéristiques biologiques propres.

Les données génétiques renvoient à ce que l'on désigne souvent comme la « science de l'hérédité »[354]. L'étude des données génétiques permet de définir les caractères biologiques d'une personne et de l'identifier grâce à son ADN contenant son génome, propre à chaque individu.

Les données biométriques renvoient quant à elles à une notion plus large. Il s'agit de toutes les données physiques ou biologiques qui concourent à l'identification d'un individu comme, l'ADN, les empreintes digitales...

Face aux évolutions scientifiques et à l'émergence de nouvelles données probatoires dans le procès se pose la question de la preuve par les données génétiques (1°) et le potentiel recours au portrait robot génétique (2°).

1° La preuve par les données génétiques

120. Bref historique – Le lien entre ADN[355] et hérédité a été découvert au milieu du 19e siècle par plusieurs scientifiques[356]. Suite aux travaux du généticien Alec Jeffreys en 1985 le recours à l'ADN est envisagé en matière criminelle. En 1987, l'expertise ADN permet de

[351] E. Truilhé-Marengo, Preuve scientifique, preuve juridique, Larcier, 2011. L'auteure rappelle néanmoins la relativité de la science qui évolue.

[352] C'est le cas par exemple du contentieux lié aux antennes relai. Il a pu être ordonné par le juge que certaines soient démontées au nom du principe de précaution.

[353] Notamment s'agissant du contentieux relatif au développement de la sclérose en plaques suite à la vaccination contre l'hépatite B. La science n'ayant jamais apporté la preuve du lien de causalité. E. Truilhé-Marengo, Preuve scientifique, preuve juridique, *op. cit.*

[354] PH. L'Héritier, Ou en est la science de l'hérédité ?, *Revue des deux mondes*, juin 1950, 47, p. 267-285.

[355] ADN pour acide désoxyribonucléique.

[356] James Watson et Francis Crick découvrent la structure de l'ADN en 1953 reprenant les travaux de Rosalind Franklin et Oswald Theodore Avery et de Johann Gregor Mendel relatifs aux principes d'hérédité biologique. Par la suite, le généticien Alec Jeffreys observera que l'ADN varie d'un individu à l'autre permettant ainsi son utilisation en criminalistique dans l'identification des individus.

confondre pour la première fois un individu[357]. Les avancées technologiques ont ensuite permis une meilleure analyse des traces ADN, notamment grâce à la découverte de Kary Mullis en 1984 qui permettra de lire l'ADN d'une seule cellule[358]. Par la suite, les techniques vont encore se développer jusqu'à permettre l'analyse de traces anciennes. Ces évolutions vont s'avérer très bénéfiques en matière criminelle notamment et seront de plus en plus utilisées au cours de procédures. L'expertise génétique est marquée par la création en 1998 du fichier national des empreintes génétiques (FNAEG) qui permet le fichage de profils recueillis sur les lieux de délits ou crimes. Constitutives de nouvelles preuves, ces données sont par nature personnelles car elles touchent directement l'identité et l'identification des individus par leur patrimoine génétique. Se posent alors les questions de l'utilisation de telles données dans le procès civil et pénal.

121. La force probante de l'ADN en matière civile – L'ADN vise à établir un lien de filiation. Il faut revenir sur les arrêts de la Cour européenne des droits de l'Homme de 2014 qui apportent une réponse à la question de la force probante de l'ADN en la matière. Dans l'affaire *A.L. contre Pologne* du 18 février 2014[359], un homme souhaitait contester son lien de filiation. L'action étant prescrite il a saisi le procureur après qu'un test ADN ait confirmé qu'il n'était pas le père biologique de l'enfant. Les juges avaient alors rejeté l'action en contestation de paternité. La Cour EDH a considéré que le rejet de l'action ne violait pas les droits et libertés fondamentaux et qu'il est nécessaire d'assurer la protection de l'intérêt supérieur de l'enfant. En effet, la Cour EDH a estimé que le fait que l'enfant ne souhaitait pas voir cette paternité contestée et au vu du temps durant laquelle elle avait été effective, l'action devait être rejetée afin de maintenir le juste équilibre entre les intérêts de l'enfant et la sécurité juridique. Dans un second arrêt du même jour, *Ostace contre Roumanie*[360], la Cour européenne des droits de l'homme a retenu que le refus de contester la filiation paternelle violait l'article 8 de la Convention. En l'espèce, l'action était intentée par l'enfant et la filiation initiale avait été prononcée par le juge et non inscrite à la demande du père comme dans la première affaire. Il ressort de ces arrêts que l'ADN ne peut à lui seul suffire à établir le lien de filiation.

[357] Dans l'affaire dite « Colin Pitchfork », les analyses génétiques réalisées à partir de sperme retrouvé sur deux victimes de viol et meurtre avaient permis de rapprocher les deux affaires et plus tard d'identifier l'auteur des crimes après avoir prélevé près de 4500 profils.
[358] Kary Mullis invente en 1984 la technique du « Polymerase Chain Reaction » permettant une analyse ADN à partir d'une seule cellule. Cette technique d'amplification permettra des expertises plus rapides.
[359] Cour E.D.H., 18 février 2014, *A.L. c/ Pologne*, n°28609-08.
[360] Cour E.D.H., 18 février 2014, *Ostace c/ Roumanie*, n°12547/06.

122. La force probante de l'ADN en matière pénale – Les analyses ADN ont permis de grandes avancées judiciaires, rendant notamment possible l'identification des auteurs d'affaires anciennes. En matière pénale, le recours à l'ADN facilite donc l'identification d'individus par le rapprochement entre le profil établi à partir de traces laissées sur les lieux de l'infraction et un profil enregistré et conservé au sein d'une base de données. Il s'agit du fichier national des empreintes génétiques (FNEAG)[361] dans lequel sont conservés tous les profils génétiques recueillis au cours d'une enquête, d'une instruction ou suite à une condamnation. La loi du 3 juin 2016[362] est venue étendre le champ d'utilisation de l'ADN permettant de trouver les auteurs en identifiant un de ses proches dans le fichier. Il s'agit de la recherche dite en « parentèle » ou de « recoupements familiaux »[363]. Si par principe tout prélèvement doit être consenti par la personne visée[364] le refus de prélèvement constitue une infraction pénale[365]. Les prélèvements peuvent être ordonnés par un officier de police judiciaire au cours d'une enquête ou sur réquisition du procureur de la République ou du juge d'instruction en matière d'infractions visées à l'article 706-55 du code de procédure pénale (notamment les infractions sexuelles et violentes, les vols et escroqueries par exemple)[366] . Une étude menée en Meurthe et Moselle et portant sur les dix années d'utilisation du FNAEG a mis en exergue certes le caractère déterminant que peut avoir l'ADN en tant que preuve dans le procès mais aussi certaines limites. Le rapport publié en mars 2017 expose que

[361] V. *infra* n° 180 s.

[362] Loi n° 2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale.

[363] Loi n°2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale. Art. 706-56-1-1 du code de procédure pénale. Cette technique permet lorsque que des traces recueilles ne permettent pas directement d'identifier l'auteur d'une infraction, d'identifier éventuellement un de ses proches fichés au FNAEG et de remonter jusqu'à lui.
C. Riccardi, L. Richefeu, Les nouvelles utilisations de la génétique dans le cadre de la procédure pénale, *RSC*, 2018, p. 331. Les auteures qualifient néanmoins cette technique de « risquée ». Elles soulèvent la question d'un risque de discriminations engendré par un ciblage sur certaines populations ainsi que du manque d'efficacité de la technique au vu notamment du nombre croissant de profils fichés.
Voir, L. Viard-Guillot, Le traitement judiciaire des infractions liées aux stupéfiants en 2015, *Bulletin d'informations statistiques du ministère de la Justice*, mars 2017, n° 150, p. 2.

[364] Art. 16 et suivants du code civil.

[365] Art. 706-56 al 2 du code de procédure pénale *« Le fait de refuser de se soumettre au prélèvement biologique prévu au premier alinéa du I est puni d'un an d'emprisonnement et de 15 000 euros d'amende.*
Lorsque ces faits sont commis par une personne condamnée pour crime, la peine est de deux ans d'emprisonnement et de 30 000 euros d'amende.
Nonobstant les dispositions des articles 132-2 à 132-5 du code pénal, les peines prononcées pour les délits prévus au présent article se cumulent, sans possibilité de confusion, avec celles que la personne subissait ou celles prononcées pour l'infraction ayant fait l'objet de la procédure à l'occasion de laquelle les prélèvements devaient être effectués.
Le fait, pour une personne faisant l'objet d'un prélèvement, de commettre ou de tenter de commettre des manœuvres destinées à substituer à son propre matériel biologique le matériel biologique d'une tierce personne, avec ou sans son accord, est puni de trois ans d'emprisonnement et de 45 000 euros d'amende ».

[366] Initialement, le FNAEG avait pour but de conserver les empreintes génétiques des auteurs d'infractions sexuelles. Son utilisation a par la suite été étendue à d'autres infractions. V. *infra* n°180 s.

concernant le territoire étudié seuls 0,5% des auteurs sont identifiés grâce à leur ADN et rappelle que ce dernier n'est pas infaillible notamment en raison du nombre important de profils fichés au FNAEG[367]. Ce dernier point soulève aussi la question des prélèvements de masse[368].

2° Le portrait robot génétique

123. Admission jurisprudentielle – S'agissant des évolutions du recours à la génétique dans le procès, il convient de s'intéresser à la question du portrait robot génétique. Ce procédé repose sur l'étude des caractéristiques génétiques à partir d'une trace recueillie sur le lieu d'une infraction. Cette analyse permet de définir par exemple la couleur des yeux, des cheveux, l'âge de la personne et d'établir ainsi un portrait robot. Cette technique n'est toutefois pas autorisée en France comme mode de preuve mais peut seulement permettre l'orientation des poursuites.

Le ministère de la justice s'est prononcé contre la mise en œuvre d'un tel dispositif, interdisant aux juges d'y avoir recours[369]. Toutefois, la chambre criminelle de la Cour de cassation dans un arrêt du 25 juin 2014[370] semble consacrer le recours à cette pratique, du moins entrouvre la porte. Dans cette affaire, le juge d'instruction a ordonné qu'il soit procédé à une analyse de traces laissées sur les lieux du crime afin de déterminer les caractéristiques génétiques de l'auteur des faits et de faciliter son identification. La Cour de cassation a estimé que ce procédé ne portait pas atteinte à la protection du corps humain puisque, précisément, les analyses avaient été effectuées à partir d'éléments détachés du corps et laissés sur les lieux. Cette décision laisse entrevoir une légiférération prochaine sur le sujet permettant peut être le recours au portrait robot génétique comme c'est le cas aux Pays-Bas par exemple. Cette pratique qui pourrait permettre une meilleure identification des auteurs d'infractions par la preuve génétique soulève néanmoins les mêmes interrogations que les utilisations déjà existantes en termes notamment de fiabilité de telles preuves et de force probante.

---

[367] V. *infra* n°180 s.

[368] Aucune disposition expresse du code de procédure pénale ne permet le recours aux prélèvements de masse. Ce procédé a pu être utilisé sur le fondement de l'article 706-54 du code de procédure pénale permettant de comparer le profil recueilli avec celui de toute personne suspecte. Ce fondement a toutefois fait l'objet de critiques.

A ce sujet, voir, M. Nicolas-Gréciano, Présentation de la législation en matière génétique, *AJ Pénal*, 2018, p. 60.

[369] Circulaire n°°08-28 du 2 juin 2011.

[370] Cass., crim., 25 juin 2014, *pourvoi* n°13-87.493.

C. Riccardi, L. Richefeu, Les nouvelles utilisations de la génétique dans le cadre de la procédure pénale, *op. cit*, p. 331.

M. Nicolas-Gréciano, Présentation de la législation en matière génétique, *op. cit.*, p. 60.

Au delà de l'ADN, les évolutions scientifiques et technologiques laissent une place grandissante de la biométrie dans le procès.

B. Les potentielles évolutions quant au recours aux données biométriques dans le procès

124. Notion d'identification faciale – A mesure que la science évolue, elle permet de nouvelles avancées en termes d'identification des individus. Plusieurs techniques d'identification biométriques semblent évoluer mais nous nous intéresserons plus spécifiquement à l'identification faciale par logiciels de reconnaissance. L'identification faciale renvoie au dispositif permettant d'identifier un individu à partir des traits de son visage que ce soit sur une image fixe ou sur une vidéo. Il s'agit dans les faits de créer un logiciel capable à partir d'une image de confondre une personne dont le profil est déjà enregistré dans une base de données, permettre ainsi son identification et prouver sa présence dans un lieu donné à un moment précis. A mi chemin entre la science et le numérique, l'identification faciale renvoie directement aux caractères biométriques de l'individu et ce même si le dispositif permettant cette identification est attaché au numérique. L'article 4 § 14 du règlement sur la protection des données définit les données biométriques comme des données *« relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique, qui permettent ou confirment son identification unique »*.

125. Avis de la CNIL quant au recours au procédé d'identification faciale – La CNIL a rendu le 15 novembre 2019 un rapport relatif à la mise en œuvre de dispositifs de reconnaissance faciale[371]. En raison du caractère sensible des données concernées et des atteintes éventuelles en termes de droits fondamentaux, la Commission appelle à un débat sur la question du recours à de tels dispositifs. La CNIL définit ce dispositif comme « une technique informatique et probabiliste qui permet de reconnaître automatiquement une personne sur la base de son visage, pour l'authentifier ou l'identifier »[372]. Elle alerte sur

[371] Voir à ce sujet, C. Crichton, Reconnaissance faciale : quels sont les enjeux à prendre en compte ?, *Dalloz Actualité*, 22 novembre 2019.

[372] CNIL rapport du 15 novembre 2019. La Commission distingue donc deux enjeux pour la reconnaissance faciale. Dans un premier temps l'authentification des individus c'est-à-dire que le dispositif permet d'apporter la preuve qu'un individu est bien celui qu'il prétend être. Dans un second temps, le dispositif permet l'identification d'un individu permettant ainsi de retrouver un individu ou de connaitre son état civil à partir de son visage. C'est cette seconde fonction qui soulève davantage de questions et appelle à plus de prudence. Si l'authentification trouve à s'appliquer à l'usage domestique ou en matière d'accès à des services, l'identification par reconnaissance faciale permet un plus grand nombre d'usages.

l'étendue des utilisations qui peuvent être faites de techniques d'identification par reconnaissance faciale (recherche d'une personne, suivi de ses déplacements…). La Commission demande qu'une analyse de mesure des risques engendrés par de telles pratiques soit réalisée dans le cadre d'une étude d'impacts. Les données biométriques étant qualifiées de « sensibles » par le règlement général sur la protection des données, leur traitement est par principe interdit sauf exceptions. Un cadre strict devra donc être posé avant tout recours à de tels dispositifs. De par l'ampleur que pourrait prendre la mise en œuvre de tels procédés, la Commission appelle à une grande prudence, parlant même de risque pour « l'anonymat dans l'espace public ». La CNIL s'est d'ailleurs déjà prononcée contre un projet dans lequel il était envisagé d'expérimenter dans une école un portail de contrôle d'accès par reconnaissance faciale des élèves, cette dernière estimant l'atteinte au droit au respect de la vie privée disproportionnée[373]. Ainsi, la CNIL recommande que toute expérimentation en la matière soit strictement encadrée dans le respect des droits de la personne.

Si la reconnaissance faciale semble promettre une meilleure identification des individus, les avancées scientifiques semblent accorder une place particulière à l'identification par d'autres données biométriques telles que les caractéristiques de l'œil ou la voix[374].

La preuve par les données scientifiques constitue donc une avancée majeure dans l'identification des individus mais soulève des interrogations quant aux potentielles évolutions qu'elle pourrait connaitre. Si la science a connu de fortes évolutions, le numérique constitue également une avancée dans le fonctionnement de la justice et dans la gestion des données probatoires. Se pose alors la question de la valeur probante d'une donnée numérique.

§2. La valeur probante des données numériques

126. Notion de donnée numérique – A l'ère du *big data* et de *l'open data*, les données numériques entrent dans le champ de la preuve soulevant de nombreuses interrogations quant à leur utilisation au sein de la procédure judiciaire. Les développements technologiques et de

[373] Délibération CNIL AP 29 octobre 2019.
J.M. Pastor, La CNIL recadre les projets sécuritaires de deux collectivités, *Dalloz Actualité*, 5 novembre 2019.
C. Rotily , L. Archambault, Données biométriques issues d'expérimentations de reconnaissance faciale sur le territoire français : un défi à l'aune du droit 2.0 ? *Dalloz* IP/IT, 2020, p. 54.

[374] L'identification par l'œil constituerait la méthode d'identification la plus fiable. Chaque œil étant unique, l'identification par ce caractère biométrique serait plus fiable que l'ADN ou l'odontologie. Si son utilisation dans les procédures judiciaires n'est encore d'actualité, la doctrine semble commencer à y porter un intérêt particulier. Ce procédé commence à être utilisé dans certains secteurs afin d'authentifier l'identité d'un individu. Voir, J.R. Demarchi, *Les preuves scientifiques dans le procès pénal*, thèse de doctorat, droit, Université de Nice-Sophia Antipolis, 2010, 1 ère partie.

l'informatique ont engendré de nouvelles formes de criminalité et permis la mise en œuvre de nouveaux procédés de recueil de données à valeur probatoire. L'administration de la preuve a donc du s'adapter à ces évolutions. La preuve numérique renvoie à toute donnée stockée dans une mémoire informatique, mails, enregistrement numérique. Le terme de « numérique » renvoie donc à la fois aux procédés permettant la collecte, le stockage, la diffusion ou l'analyse de données et aussi à toute donné informatique, dématérialisée. C'est certainement cette multitude de visages qui fait du numérique à la fois un outil efficace mais aussi une source de risques et de menaces. Quoi qu'il en soit, le développement d'internet a poussé le législateur à intervenir notamment afin d'encadrer autant que possible le traitement des données personnelles en ligne. La question qui se pose ici est de savoir quelle est la valeur d'une donnée numérique en tant que preuve dans un procès. Le principe de liberté de la preuve et donc la libre appréciation des preuves par le juge qui domine en procédure pénale ne soulève pas d'interrogations particulières. Toutefois, dans les cas où la preuve est encadrée par les textes, la question de la force probante des données numériques soulève davantage d'interrogations.

A. L'appréciation de la preuve encadrée par la loi

127. Données personnelles et appréciation des preuves légales – Dans l'appréciation légale de la preuve qui distingue traditionnellement la preuve parfaite[375] de la preuve dite imparfaite[376], c'est la question de la force probante de l'écrit dans la preuve des actes juridiques qui intéresse le sujet du traitement des données à caractère personnel permettant par la suite un parallèle avec l'écrit numérique.
Par exception au principe de liberté de la preuve édicté à l'article 1358 du code civil, l'article 1359 impose l'écrit comme preuve d'un acte juridique dont la valeur excède 1500 euros[377].

128. Force probante de l'acte authentique – L'acte authentique doit remplir des conditions posées à l'article 1369 du code civil, qui impose un formalisme particulier et l'enregistrement

[375] La preuve est qualifiée de parfaite lorsqu'elle lie le juge qui doit dès lors l'admettre comme telle dans le procès. Voir G. Lardeux, *Preuve – modes de preuves*, Répertoire de droit civil, *op. cit*.
[376] La preuve dite imparfaite voit sa force probante dépendre de l'appréciation du juge. Certains auteurs font référence aux demi-preuves. Le terme de demi-preuve renvoie plus à un concept qu'à une notion juridique. Issu du droit médiéval, ce système a été abandonné à la révolution. La doctrine fait toutefois référence à un maintien résiduel de ces demi-preuves ces dernières engendrant une diminution de la force probante puisqu'elles doivent être corroborées par d'autres. Voir, E. Vergès, G. Vial, O. Leclerc, *Droit de la preuve, op. cit.*, p. 425.
[377] Ordonnance n° 2016-131 du 10 févier 2016 et Décret 2004-836 du 20 août 2004.

de l'acte par un officier public[378]. Cet acte enregistré par un officier public fait foi tant qu'il n'a pas fait l'objet d'une procédure d'inscription de faux[379]. Cette procédure permet de contester la véracité de l'acte en invoquant une erreur matérielle c'est à dire en apportant la preuve d'un mensonge dans la rédaction de l'acte[380]. La procédure peut aussi porter sur un « faux intellectuel »[381] renvoyant ici à l'existence de fausses déclarations dans l'acte. Ainsi, les dispositions de l'acte authentique « font foi » jusqu'à inscription de faux. Cette force probante ne s'applique néanmoins qu'aux éléments constatés par le notaire. S'agissant des éléments énoncés par les parties, ils valent preuve jusqu'à preuve du contraire[382].

129. Force probante de l'acte sous signature privée – L'acte sous signature privée ne doit répondre à aucun formalisme outre la signature de celui qui s'oblige. La force probante de l'acte sous signature privée n'est pas similaire selon que l'on appréhende les effets probatoires entre les parties ou envers les tiers. En effet, mettant un terme aux dispositions antérieures ambigües, l'article 1372 du code civil pose le principe selon lequel l'acte sous signature privée fait foi entre les parties. S'agissant de l'effet envers les tiers, l'article 1377 du code civil dispose que *« L'acte sous signature privée n'acquiert date certaine à l'égard des tiers que du jour où il a été enregistré, du jour de la mort d'un signataire, ou du jour où sa substance est constatée dans un acte* authentique». Sa force probante est donc moindre que celle de l'acte authentique[383].

B. L'appréciation de la donnée numérique

130. La reconnaissance de l'écrit numérique par le législateur – La loi du 13 mars 2000[384] érige l'écrit numérique au même rang que l'écrit papier lui accordant la même valeur

[378] Art. 1369 du code civil, *« L'acte authentique est celui qui a été reçu, avec les solennités requises, par un officier public ayant compétence et qualité pour instrumenter.*
Il peut être dressé sur support électronique s'il est établi et conservé dans des conditions fixées par décret en Conseil d'État.
Lorsqu'il est reçu par un notaire, il est dispensé de toute mention manuscrite exigée par la loi ».
[379] Art. 1371 du code civil. Art. 303 et suivants du code de procédure civile.
[380] G. Lardeux, *Preuve – modes de preuves,* Répertoire de droit civil, *op. cit*.
[381] *Ibid*.
[382] F. Ferrand, *Preuve, Le juge et la preuve écrite,* Répertoire de procédure civile, Dalloz, décembre 2013, actualisation décembre 2019.
[383] *Ibid*.
[384] Loi 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique.

probatoire[385]. Néanmoins, certaines garanties doivent être apportées. La personne qui a rédigé l'écrit numérique doit être identifiée et l'intégrité du document doit être conservée.

131. Les caractères spécifiques attachés à la preuve numérique – Aux côtés des principes de loyauté et de proportionnalité dans le recueil, la preuve numérique soulève des interrogations spécifiques liées à sa nature. A ce sujet, l'article 1367 du code civil définit la signature électronique comme *« un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache. La fiabilité de ce procédé est présumée, jusqu'à preuve contraire, lorsque la signature électronique est créée, l'identité du signataire assurée et l'intégrité de l'acte garantie, dans des conditions fixées par décret en Conseil d'Etat »*.

132. De la donnée numérique à la preuve – Finalement, avant d'être une preuve dans le procès, il est question d'une donnée numérique. Cette donnée doit remplir certains critères[386] afin de pouvoir prétendre à une valeur probante dans le procès et sa nature même impose de remplir certaines conditions. En effet, la donnée numérique est « volatile » et donc « vulnérable »[387]. Le premier critère est celui de l'authenticité qui permet de pouvoir rattacher avec certitude la donnée à un individu et donc de garantir sa provenance. Le second critère est celui de l'intégrité qui permet d'avoir connaissance de toute modification éventuelle, même infime d'un fichier, ce dernier laissant alors une « empreinte numérique » différente. Ce critère d'intégrité garanti donc le contenu du fichier informatique. Enfin le critère de traçabilité permet de suivre le fichier quant bien même il aurait fait l'objet de copie sur différents supports. Enfin la donnée doit nécessairement être exploitable. Tous ces critères ajoutés aux conditions classiques d'admissibilité de la preuve font de la preuve numérique une preuve par nature « complexe »[388]. Cette complexité a donné lieu à de nombreux débats et contentieux. A titre d'exemple, la question de la preuve numérique dans le procès s'est posée s'agissant des données présentes sur les réseaux sociaux. A ce sujet, la Cour de cassation a du se prononcer à plusieurs reprises sur la question de l'admissibilité de preuves rapportées par la présentation de données issues de réseaux sociaux. La question sous jacente est de savoir si les conversations menées sur un réseau social et les informations échangées par ce biais sont

[385] Art. 1316-3 du code civil.
[386] Critères exposés par M. Serge Migayron lors d'un colloque relatif à la preuve numérique, Colloque, La preuve numérique à l'épreuve du litige, Cour d'appel de Paris, 13 avril 2010.
[387] M. Serge Migayron lors d'un colloque relatif à la preuve numérique à l'épreuve du litige le 13 avril 2010, Compte-rendu du colloque, p. 22, 23.
[388] Par exemple, M. Clément-Fontaine, colloque relatif à la preuve numérique à l'épreuve du litige le 13 avril 2010, Compagnie nationale des experts de justice en informatique et techniques associées.

privées ou non et dans quelle mesure elles sont utilisables librement en justice comme mode de preuve. En matière civile, la Cour d'appel de Limoges a jugé recevable la reproduction de propos tenus sur Facebook pour apporter la preuve du manque de maturité d'une mère et donc de son incapacité à assumer ses obligations découlant de l'autorité parentale sur son enfant[389]. Aussi, dans une procédure de divorce, la Cour d'appel de Douai a estimé que la production de propos tenus sur sa page Facebook pouvaient être utilisés comme preuve d'une faute d'adultère[390]. Ce raisonnement a été confirmé par la suite dans d'autres affaires par la Cour de cassation qui a considéré que le fait d'échanger sur un réseau social avec une tierce personne des mails équivoques et des photos intimes caractérise une faute justifiant le divorce aux torts exclusifs de la personne à l'origine de ces messages[391].

Conclusion du titre 1

133. L'application classique du droit de la preuve – Le traitement des données à caractère personnel dans les procédures judiciaires impose de s'interroger sur leur collecte en tant que preuves. Le constat premier est celui de l'application classique des principes régissant le droit de la preuve avec peu de référence à la preuve en tant
que données à caractère personnel ou peu de spécificités attachée à la nature « personnelle » des données. Toute donnée probatoire collectée dans une procédure est par définition une donnée à caractère personnel mais cette « reconnaissance » n'amène dans l'immédiat pas une application différente des principes encadrant la preuve.

134. Approche au regard du caractère sensible des données – Néanmoins, cette approche amène à porter un regard particulier sur les procédés de collecte notamment lorsqu'il s'agit de données sensibles au sens de la loi informatique et libertés. La CNIL a, à ce sujet, parfois alerté sur les risques de certains modes de collecte au vu de la vie privée mais aussi de la nature des données à caractère personnel concernées. L'approche du droit de la preuve au regard du droit des données permet donc d'adopter un regard plus protecteur de la donnée elle-même et non pas seulement en termes de vie privée de la personne.

[389] CA Limoges, 30 mars 2011, RG 10/00383. La Cour d'appel a estimé que les propos rapportés traduisaient le « caractère inconstant, inconséquent et désinvolte » ainsi que l' « immaturité » et « l'instabilité » de la mère de l'enfant, décidant ainsi de fixer la résidence habituelle de l'enfant chez son père.
[390] CA Douai, 14 mars 2013, RG 11/06457.
[391] Cass., 1 ère civ., 30 avril 2014, *pourvoi* n ° 13-16.649.

135. La nécessaire adaptation des textes – Le second constat est celui de la nécessaire adaptation des textes aux nouvelles preuves et notamment aux évolutions numériques et scientifiques. La reconnaissance de l'écrit numérique au même titre que l'écrit papier marque une étape importante dans l'admission des données numériques comme preuves dans les procédures.

Que ce soit du fait de l'émergence des nouveaux moyens de communication ou du fait des évolutions scientifiques, le législateur a du adapter les règles existantes afin de permettre la collecte de ces données dans le respect du droit de la preuve et, plus récemment du droit de la protection des données.

TITRE 2 : LES DONNEES A CARACTERE PERSONNEL ALIMENTANT DES FICHIERS JUDICIAIRES

136. Notions – La notion générale de fichier judiciaire ou celle de fichier de police ne trouve pas de définition stricte dans la loi. La loi informatique et liberté fait référence aux traitements de données à caractère personnel mis en œuvre pour le compte de l'Etat ayant pour objet la prévention, recherche, constatation ou poursuite des infractions pénales[392]. De manière plus générale, le règlement européen sur la protection des données vise la catégorie de données relatives aux condamnations pénales et aux infractions dans son article 10, qui justifie que soit fixé un cadre spécifique. Le législateur encadre les fichiers et leurs traitements de manière individuelle. Cette notion de fichier renvoie en ce qui concerne le traitement de données lors de procédures judiciaires aux fichiers « de police »[393].

137. Les fichiers judiciaires une catégorie hétérogène – Les fichiers judicaires de par leur hétérogénéité renvoient davantage à une notion qu'à une catégorie juridique stricte[394]. La notion de fichier de police est utilisée par facilité mais le terme même peut être discuté. En effet, sous ce vocable sont regroupés grand nombre de fichiers qui obéissent à des règles de création, de traitement différents et qui sont également soumis à des autorités de contrôle différentes. Les textes font également référence aux traitements de données à caractère personnel intéressant la sûreté de l'Etat et la défense, pour lesquels des dispositions spéciales et dérogatoires sont prévues. Ces fichiers ont été listés dans un décret du 15 mai 2007[395] et regroupent des fichiers relevant tant du renseignement que du ministère de la justice ou du ministère de la défense. Ils renvoient à la notion de fichiers de « souveraineté ». Il est parfois fait référence aux fichiers de police quant à la nature des données contenues dans les fichiers en question. Il faut néanmoins garder à l'esprit que les données qui interviennent dans les procédures judiciaires peuvent également être issues de fichiers de renseignement

[392] Art. 31 de la loi informatique et libertés
[393] P.Y Marot, Fonction et mutation des fichiers de police, *AJ Pénal*, 2007, p. 61.
[394] D. Larbre, « Les fichiers de police : une catégorie juridique incertaine ? », *Terminal, technologie de l'information*, culture et société, 108-109, 2011, p. 141 à 151. Cette idée est mise en avant dans l'ouvrage cité. Une catégorie juridique renvoyant un à régime s'appliquant à un objet donné, l'on ne peut pas parler de « catégorie juridique » concernant les fichiers de police, ces derniers renvoyant à de nombreux régimes et constituant un ensemble très hétérogène. L'auteur fait également le constat de la remise en cause par la doctrine de la notion même de fichier de police.
[395] Décret 2007-914 du 15 mai 2007 pris pour l'application du I de l'article 30de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

administratifs[396]. L'utilisation de telles données dans le procès tend nécessairement à faire de ces dernières des données judiciaires par finalité. Ces fichiers renvoient en réalité aux différents systèmes automatisés de gestion d'informations à vocation « opérationnelle »[397] utilisés lors des enquêtes notamment. Sous l'appellation de « fichiers judiciaires » sont rassemblés tous les outils de recueil et de traitement de données automatisés utilisés pour le compte de la justice et par grand nombre de ses acteurs. Qu'il s'agisse de données relatives aux procédures en cours, aux personnes liées à ces procédures ou aux éventuelles données susceptibles de constituer des indices futurs, ces fichiers regroupent des données multiples et de natures variées. En réalité ces fichiers rassemblent tous les systèmes de traitement de données susceptibles d'intervenir au cours de procédures judiciaires. Il semble opportun d'utiliser le terme de « fichiers judiciaires », qui englobe de fait à la fois les fichiers de police, les fichiers judiciaires et par extension les fichiers de renseignement susceptibles d'intervenir dans les procédures judiciaires.

138. Définition des fichiers judiciaires et de police par la CNIL – Du point de vue de la Commission nationale de l'informatique et des libertés (CNIL), la notion de fichier judiciaire et de police renvoie au traitement de données à caractère personnel tel qu'il en est fait référence dans l'article 2 de la loi informatique et libertés du 6 janvier 1978[398]. La CNIL fait directement référence à la notion de traitement de données. S'agissant des fichiers judiciaires, la loi informatique et libertés fait référence au traitement de données « mis en œuvre pour le compte de l'Etat ». Ainsi, l'article 31[399] de la loi encadre ces traitements et les définit en

[396] V. Gautron, *Fichiers de police*, Répertoire de droit pénal et de procédure pénale, avril 2015, actualisation mars 2019, 107. L'auteure fait référence à la « double finalité » de certains fichiers, les procédures judiciaires faisant parfois appel aux données de fichiers administratifs et inversement.

[397] A. Bauer, C. Soullez, M. Ventre, *Mieux contrôler la mise en œuvre des dispositifs pour mieux protéger les libertés*, La documentation française, coll. Des Rapports officiels, 2008, p.15.

[398] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés dite « LIL ». Art 2 *« La présente loi s'applique aux traitements automatisés en tout ou partie de données à caractère personnel, ainsi qu'aux traitements non automatisés de données à caractère personnel contenues ou appelées à figurer dans des fichiers, lorsque leur responsable remplit les conditions prévues à l'article 3 de la présente loi, à l'exception des traitements mis en oeuvre par des personnes physiques pour l'exercice d'activités strictement personnelles ou domestiques.*
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.
Sauf dispositions contraires, dans le cadre de la présente loi s'appliquent les définitions de l'article 4 du règlement (UE) 2016/679 du 27 avril 2016 ».

[399] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés dite « LIL ». Art 31 *« I.- Sont autorisés par arrêté du ou des ministres compétents, pris après avis motivé et publié de la Commission nationale de l'informatique et des libertés, les traitements de données à caractère personnel mis en oeuvre pour le compte de l'Etat et :*
1° Qui intéressent la sûreté de l'Etat, la défense ou la sécurité publique ;

fonction de leur finalité. Au sens de la loi informatique et libertés, constitue un fichier judiciaire tout traitement mis en œuvre pour le compte de l'Etat ayant pour finalité la sûreté de l'Etat, la défense ou la sécurité publique ; ou la prévention, la recherche ou la constatation des infractions pénales. Ces traitements doivent obéir à une réglementation particulière. La notion de fichier peut être, en la matière, plus extensive encore.

139. Etat des lieux – Un rapport d'information déposé par la Commission des lois en 2018 s'est intéressé aux « fichiers mis à la disposition des forces de sécurité ». Cette étude visait les fichiers utilisés par les services de police et de gendarmerie ainsi que les services rattachés au ministre de l'intérieur remplissant des missions de renseignement. La notion de fichier développée dans ce rapport dépasse donc le cadre de l'article 31 de la loi informatique et libertés. Ce rapport fait état de 106 fichiers. Les fichiers de police ont été souvent qualifiés de « catégorie juridique incertaine »[400] et de manière générale et récurrente, ils sont présentés comme des outils de prévention et de répression des infractions[401]. Le nombre de fichiers a évolué de manière exponentielle. L'utilisation et plus généralement le traitement des données fichées soulèvent de vives critiques et inspire beaucoup de craintes. Différents « scandales » ont frappés l'opinion publique et fait réagir ; comme notamment l'affaire dite du « projet SAFARI »[402] en 1973 qui donna lieu à la création par le Gouvernement de l'époque de la CNIL et plus récemment, du scandale «PRISM » qui révéla le fichage par les organismes gouvernementaux américains de données détenues par les serveurs du web[403].

2° Ou qui ont pour objet la prévention, la recherche, la constatation ou la poursuite des infractions pénales ou l'exécution des condamnations pénales ou des mesures de sûreté.
L'avis de la commission est publié avec l'arrêté autorisant le traitement.
II.-Ceux de ces traitements qui portent sur des données mentionnées au I de l'article 6 sont autorisés par décret en Conseil d'Etat pris après avis motivé et publié de la commission. Cet avis est publié avec le décret autorisant le traitement.
III.-Certains traitements mentionnés au I et au II peuvent être dispensés, par décret en Conseil d'Etat, de la publication de l'acte réglementaire qui les autorise. Pour ces traitements, est publié, en même temps que le décret autorisant la dispense de publication de l'acte, le sens de l'avis émis par la commission.
IV.-Pour l'application du présent article, les traitements qui répondent à une même finalité, portent sur des catégories de données identiques et ont les mêmes destinataires ou catégories de destinataires peuvent être autorisés par un acte réglementaire unique. Dans ce cas, le responsable de chaque traitement adresse à la commission un engagement de conformité de celui-ci à la description figurant dans l'autorisation.».

[400] Voir par exemple, D. Larbre, « Les fichiers de police : une catégorie juridique incertaine ? », *op. cit.*, pp. 141-151.

[401] Voir par exemple, A. Decocq, J. Montreuil, J. Buisson, *Le droit de la police*, Litec, 1998, p. 731. Les auteurs font ici référence à « des instruments de recherche utilisés à des fins de prévention et répression d'infraction ».

[402] SAFARI : système informatisé pour les fichiers administratifs et le répertoire des individus.

[403] PRISM du nom du fichier utilisé par la NSA et le FBI permettant de collecter des données personnelles au niveau mondial par le biais des serveurs internet. Cette affaire a été révélée dans la presse par E. Snowden en 2013. En France, plusieurs organismes (LDH et FIDH) ont déposé une plainte contre X le 11 juillet 2013 pour atteintes à la vie privée, collecte frauduleuse de données personnelles, accès frauduleux à un système de

140. L'établissement d'une nomenclature relative aux fichiers judiciaires et de renseignement – L'étude des fichiers et des normes encadrant leur création suppose de fixer une nomenclature permettant leur présentation. En s'appuyant sur les différents rapports rendus en la matière, l'adoption du critère fonctionnel semble le plus opportun. Dans le rapport BAUER de 2008 établi sous la direction d'Alain Bauer, le groupe de travail a fait ressortir l'existence de huit catégories de fichiers. Le rapport vise les fichiers de « police et gendarmerie »[404].

Il distingue tout d'abord les « applications bureautiques » qui sont des outils permettant, par exemple, le traitement administratif des procès-verbaux[405], des interventions[406], des prélèvements biologiques[407] ou encore qui permettent l'enregistrement et le suivi des procédures[408].

Ensuite, le rapport vise les « fichiers administratifs » tels que le fichier de la batellerie[409], le fichier des passagers aériens[410] (FPA) ou le fichier national transfrontière[411] (FNT) qui ont de manière générale vocation à recenser des données purement administratives relatives à une catégorie de personnes donnée. Ces données trouvent néanmoins parfois à être utilisées lors de procédures judiciaires.

---

traitement automatisé de données et utilisation, conservation de données obtenues par des moyens frauduleux et atteinte au secret des correspondances.

[404] Il ressort de la réflexion du groupe de travail huit catégories de fichiers de police et gendarmerie : les applications bureautiques, les fichiers administratifs, les fichiers à vocation judiciaire, les fichiers de renseignement, les fichiers d'antécédents judiciaires, les fichiers d'identification judiciaire, les systèmes de traitement du renseignement judiciaire et les fichiers d'identification administrative.

[405] Par exemple l'application Bureautique Brigade 2000 (BB2000) crée par arrêté ministériel du 28 octobre 1992 et contenant des informations relatives aux personnes impliquées dans des procédures ou ayant été condamnées au paiement d'une amende forfaitaire par exemple. Cette application a été remplacée en 2009 par l'application Pulsar.

[406] Par exemple, l'application ARAMIS servant de relais entre les brigades et compagnies de gendarmerie et leur hiérarchie. Cette application a été remplacée en 2009 par l'application ATHEN@.
Le LPR (logiciel de rédaction de procédures) permet la rédaction automatisée des procès-verbaux.
Aussi, le logiciel Ic@re, permet la rédaction de procès-verbaux par les agents de l'armée et de la gendarmerie.

[407] Le fichier de gestion du service central de préservation des prélèvements biologiques (SCPPB) créé par arrêté ministériel du 13 septembre 2002 permet la gestion des traces biologiques collectées dans le cadre de procédures.

[408] S'agissant de telles applications, il convient de citer CASSIOPEE[408]. Cette application a été mise en œuvre dans les tribunaux de grande instance suite au décret du 18 juin 2010[408]. Elle permet l'enregistrement des procédures par les bureaux d'ordre des Parquets et le suivi entre les différents intervenants (magistrats, police, gendarmerie...). Elle conserve ainsi une trace de toute la chaîne pénale de l'enregistrement de la plainte au prononcé du jugement.

[409] Le fichier de la batellerie créé en 1942 a été supprimé en 2010.

[410] Le fichier des passagers aériens créé par la loi du 23 janvier 2006 et son décret d'application n°1630-2006 du 19 décembre 2006, découle de l'obligation instaurée par l'article 7 de la loi du 23 janvier 2006 relative à la lutte contre le terrorisme. Cette dernière impose aux compagnies aériennes de collecter les données personnelles relatives aux passagers. Le but est de prévenir les actes terroristes et de mieux les réprimer. Ce fichier est interconnecté avec le fichier des personnes recherchées (FPR) et le Système d'information Schengen (SIS).

[411] Le fichier national transfrontière (FNT) créé par arrêté ministériel du 29 août 1991 et modifié par arrêté du 3 novembre 2006 s'inscrit dans la loi du 23 janvier 2006 relative à la lutte contre le terrorisme. Il permet d'améliorer le contrôle aux frontières pour mieux prévenir les actes terroristes.

« Les fichiers à vocation judiciaire » comme par exemple le fichier national du faux monnayage (FNFM)[412], le fichier des véhicules volés[413] ou le Système d'information Schengen créé à la suite de l'accord Schengen[414]. Ces fichiers à vocation judiciaire recensent des informations relatives à des procédures ou des personnes impliquées dans des types d'affaires données (tels que le vol de véhicule ou le faux monnayage) ainsi que des renseignements qui pourraient avoir un lien avec ces affaires.

« Les fichiers de renseignement » comme par exemple le fichier CRISTINA[415] ont vocation à contenir des informations à destination des services de renseignement et sont par principe accessibles à des personnes spécialement habilitées[416].

« Les fichiers d'antécédents » ont comme leur nom l'indique vocation à conserver des informations relatives aux condamnations et infractions. Ils trouvent une utilité en matière de prévention des infractions et de répression. Ce sont particulièrement ces fichiers qui soulèvent des interrogations en matière de traitement de données à caractère personnel. A titre d'exemple on peut citer le traitement des antécédents judiciaires[417] (TAJ) qui recense des données relatives aux mis en cause et victimes d'infractions. C'est un des fichiers les plus utilisés en matière d'enquêtes judiciaires et administratives et un de ceux qui recense le plus d'individus. « Les fichiers d'identification judiciaire » ont également une grande utilité lors des enquêtes. Ils sont régulièrement source de critiques et d'inquiétudes tant sur le nombre de personnes visées que sur la nature des données conservées ou encore sur leur utilisation même. Il s'agit par exemple du fichier judiciaire national automatisé des auteurs d'infractions sexuelles[418] (FIJAIS) qui recense l'identité des personnes condamnées, même non définitivement, pour des faits d'infractions sexuelles et d'autres crimes violents. Ce fichier a clairement une utilité quant à l'identification d'auteurs d'infractions et également en matière de prévention de la récidive. Dans cette catégorie de fichiers s'inscrit également le fichier

[412] Il a été créé en 2002 après l'adoption de la monnaie européenne et répond aux obligations imposées par le règlement européen 1338/2001 du 28 juin 2001 relatif à la protection de l'euro contre le faux monnayage. Il a vocation à recenser les affaires liées au faux monnayage.

[413] Créé par arrêté du 15 mai 1996 et modifié en 2005.

[414] Le fichier d'information Schengen découle de l'accord Schengen et son décret d'application n°95-577 du 6 mai 1995. Il est alimenté par le fichier des véhicules volés ainsi que par le fichier des personnes recherchées.

[415] CRISTINA (centralisation du renseignement intérieur pour la sécurité du territoire et les intérêts nationaux). Ce fichier est couvert par le secret défense, son décret d'application n'a donc pas été publié. Il s'agit d'un fichier dit de « souveraineté » tel que défini par la loi du 6 janvier 1978.

[416] C'était également le cas du fichier EDVRISP[416] qui contient des données relatives aux personnes dont l'activité pourrait constituer une menace pour la sécurité publique. Ce dernier a néanmoins été abandonné et ses dispositions ont été reprises au sein d'autres dispositifs.

[417] Le TAJ (traitement des antécédents judiciaires), remplace en 2012 les fichiers JUDEX et STIC par le décret n°2012-652 du 4 mai 2012 après avis CNIL du 7 juillet 2011.

[418] Le FIJAIS est issu de la loi dite Perben I n°2004-204 du 9 mars 2004 qui a fait l'objet de nombreuses délibérations de la CNIL.

automatisé des empreintes digitales[419] (FAED) ou le fichier national des empreintes génétiques[420] (FNAEG) recensant des données digitales et génétiques permettant l'identification des auteurs d'infractions.

« Les systèmes de traitement du renseignement judiciaire » ont vocation à réaliser des analyses transversales entre les enquêtes et permettre des rapprochements afin de faciliter l'identification d'auteurs d'infractions graves[421].

Enfin, « les fichiers d'identification administrative » recensent des données concernant les documents administratifs tels que la carte d'identité, le passeport, le permis de conduire[422]. Cette catégorie bien que citée dans la liste des fichiers de police et gendarmerie par le groupe de travail n'intéresse pas particulièrement le traitement des données dans le cadre des procédures judiciaires.

141. Catégorisation des fichiers judiciaires – Un rapport d'information de la commission des lois relatif aux « fichiers de police » déposé en 2009 a en fonction de leur finalité distingué quatre catégories :

- Les fichiers à caractère administratif qui conservent des données administratives relatives à des personnes ou des objets.
- Les fichiers de police qui englobent les fichiers à vocation judiciaire, les fichiers d'antécédents et les fichiers d'identification et qui collectent et centralisent des données destinées à lutter contre les infractions et faciliter leur constatation.
- Les fichiers de renseignement qui regroupent les fichiers mis en œuvre par les services du renseignement et par le ministère de l'intérieur chargé de la sécurité intérieure.
- Enfin, les fichiers de rapprochement destinés à lutter contre la délinquance sérielle et les fichiers ou logiciels de rapprochement et d'analyse criminelle[423].

Il s'agit ici de s'intéresser aux données à caractère personnel qui font l'objet d'un fichage au cours d'une procédure judiciaire soulevant ainsi des interrogations s'agissant des normes encadrant la création de ces fichiers (Chapitre 1) et s'agissant dans un deuxième temps de

[419] Le FAED a été créé par le décret n°97-249 du 8 avril 1987, modifié en 2005.
[420] Le FNAEG a été créé par les lois du 17 juin 1998 et du 18 mars 2003 et le décret d'application du 18 mai 2000.
[421] On peut citer par exemple le SALVAC (système d'analyse et de liens de la violence associée au crime) créé par la loi du 18 mars 2003 ; ou ANACRIM créé par la loi n°2005-1549 du 12 décembre 2005 et loi n°2003-239 du 18 mars 2003.
[422] Par exemple le fichier relatif à la carte nationale d'identité, le fichier relatif aux passeports.
[423] Rapport d'information de la commission des lois constitutionnelles, de la législation et de l'administration générale de la République sur les fichiers de police, Députés BATHO D. et BENISTI J-A, déposé le 24 mars 2009.

l'échange et du partage de ces données (Chapitre 2). Plus généralement, le fichage pose la question des éventuelles atteintes en terme de libertés individuelles et notamment le respect de la vie privée ou la présomption d'innocence.

CHAPITRE 1 : LA CREATION DES FICHIERS JUDICIAIRES

142. Historique de la création des fichiers de police – La création de fichiers de police n'est pas récente. De tels fichiers ont été instaurés pour des raisons parfois d'ordre public, pour mettre en œuvre des politiques sécuritaires et aussi parfois afin de mettre en œuvre d'autres stratégies politiques parfois critiquables.

Fin 2011, les archives nationales ont réalisé une exposition photographique intitulée « fichés ?»[424]. Cette exposition a présenté des documents relatifs au fichage du second empire aux années 60. Elle rassemblait plus de 2300 documents qui permettent d'établir un historique du fichage en France. L'exposition recensait une sélection de registres, listes, dossiers, fiches et autres formes de traitement. Des simples notes préfectorales aux « fichiers juifs »[425] de Vichy, l'exposition permettait aussi de découvrir les fiches de personnages de l'histoire tel que Salvador Dali classé « contre-espionnage » ou Django Reinhardt estampillé « forain ». Etaient exposés également les fichiers de « nomades » dans lesquels les personnes sont photographiées de profil et l'oreille découverte ainsi que les premières cartes d'identité[426].

On ne peut étudier la question des fichiers de police sans aborder le « projet SAFARI »[427] qui fut la cause de l'adoption de la loi informatique et libertés le 6 janvier 1978 et de la création de la CNIL. Initié en 1973 par le ministère de l'intérieur, ce projet visait à interconnecter une grande partie des fichiers de l'Administration en identifiant les français à partir du numéro d'inscription au répertoire national d'identification (dit numéro NIR)[428]. Cette révélation souleva un grand mécontentement dans l'opinion publique et imposa au Gouvernement de réagir.

143. Les craintes soulevées par les fichiers judiciaires – La notion même de fichiers de police soulève le plus souvent la crainte au vu de différents scandales qui ont pu être révélés au cours de l'histoire. Aujourd'hui encore, certains fichiers font polémiques et sont source de

[424] Exposition « Fichés ?», *Archives nationales*, 2011.

[425] Les « fichiers juifs » encore surnommé « fichier Tulard » du nom du policier qui a établi le fichage des juifs et des communistes.

[426] Pendant longtemps, l'oreille droite était le signe distinctif utilisé pour identifier les individus avant que ce soit les empreintes digitales. Voir à ce sujet, JM. Berlière, P. Fournier, *Fiché ? Photographie et identification 1850-1960*, Perrin, 2011.

[427] SAFARI ou Système automatisé pour les fichiers administratifs et le répertoire des individus. L'information de la création de ce fichier fut révélée en 1974 par le quotidien Le Monde dans un article intitulé « Safari ou la chasse aux français ». Suite au scandale qui en découla, le législateur décida d'adopter la loi informatique et liberté et de créer une autorité administrative indépendante, la CNIL chargée du contrôle des fichiers et de la protection des données personnelles.

[428] Il s'agit du numéro INSEE ou plus simplement du numéro de sécurité sociale attribué à chaque individu à sa naissance à partir des données de l'état civil transmises à l'INSEE.

vives critiques voire même de condamnations par les juridictions internes et supra nationales[429]. Toutefois, il convient de rappeler que la création de certains de ces fichiers a permis de grandes avancées en terme de lutte contre la délinquance et la criminalité. On peut citer notamment la création du fichier national des empreintes génétiques qui a permis d'identifier des auteurs de crimes qui étaient jusqu'alors introuvables en les confondant grâce à leur ADN.

L'objectif de cette section est de s'intéresser aux motivations et aux critères justifiant la création des fichiers (section 1) pour ensuite s'interroger plus précisément sur les normes qui encadrent ces derniers (section 2). Cette analyse permettra d'un côté de faire ressortir l'utilité voir la nécessité de mettre en œuvre de tels outils tout en soulevant certaines interrogations notamment en terme de droits fondamentaux.

Section 1 : Les critères fonctionnels justifiant la création des fichiers judiciaires

144. Finalités multiples – Les fichiers judiciaires trouvent une utilité en termes de preuve mais également de prévention des infractions. De ce fait, ils rassemblent grand nombre de données. De l'identité des suspects et des victimes, à celle des personnes condamnées en passant par les traces ADN et les données biologiques, les fichiers de police regroupent des données multiples à vocations diverses. Dans le rapport du groupe de contrôle paru en 2008 sous la direction d'Alain Bauer, 45 fichiers de police et gendarmerie ont été recensés. Si l'on s'en tient à la définition large de la notion de fichiers telle qu'évoquée dans le rapport et dans le rapport de la commission des lois de 2009, ce nombre a largement augmenté depuis. Cette dernière fait état de 106 fichiers utilisés dans le cadre d'enquêtes. Il s'agira ici de s'intéresser aux fichiers intervenant lors de procédures judiciaires. Cette notion de procédure sera entendue largement, considérant que le fichage des antécédents et l'enregistrement des condamnations intéressent nécessairement la question du traitement des données à caractère personnel dans le cadre des procédures judiciaires.

145. Approche selon la finalité – Afin d'aborder ces fichiers judiciaires, il paraît intéressant de les appréhender en fonction de leur finalité. De manière générale, on peut distinguer deux catégories de traitements automatisés de données à caractère personnel, les fichiers conservant

[429] Comme récemment la censure du Conseil constitutionnel concernant la création d'un fichier central biométrique.

des données et les systèmes permettant l'exploitation transversale des données fichées. Il ressort de l'inventaire de tous les fichiers la notion de finalité et de nécessité dans le traitement mis en œuvre.

Les fichiers peuvent être présentés comme « un instrument de police par destination »[430]. Reprenant le critère de finalité ou de « l'intention »[431], M. Chambon opère une distinction entre les fichiers de police administrative « ne portant pas sur des auteurs d'infractions précises » entrant dans la mission générale de contrôle et de surveillance de l'agent et les fichiers de police judiciaires destinés à « la recherche d'une infraction précise »[432]. Il qualifie donc les fichiers « d'instruments de renseignements » ; lorsque leur but est la sécurité publique et le maintien de l'ordre public il s'agit alors « d'instruments de police ». Il faut néanmoins soulever la tendance actuelle à la disparition de la frontière entre fichier administratif et fichier judiciaire qui soulève des interrogations en termes d'utilisation des fichiers de police.

146. Approche du sujet – Afin d'appréhender le contexte ayant motivé la création des fichiers judiciaires, il peut être utile de présenter ces derniers en s'appuyant sur les différents rapports qui ont pu être établis et notamment le rapport Bauer, bien qu'aujourd'hui la distinction des fichiers en fonction de leur finalité peut être remise en cause. En effet, il s'avère que certains fichiers voient leurs finalités étendues, certaines données alimentent plusieurs fichiers par le biais d'interconnexions, notamment. Aussi, se pose la question de l'existence réelle d'une frontière entre fichiers de police judiciaire et fichiers de renseignement[433]. Suivant donc ce critère de finalité découlant des différentes nomenclatures qui ont pu être établies dans les divers rapports cités précédemment, il convient de distinguer les fichiers permettant la prévention d'infractions (§1.), les fichiers intervenant dans la constatation des infractions et le recueil de preuves (§2.), les fichiers d'identification judiciaire (§3.) et le cas particulier du casier judiciaire national qui constitue une véritable mémoire judiciaire (§4.). Enfin, les évolutions récentes soulèvent la question de la création de traitements de données judiciaires qui seraient au service de la prédictivité de la justice (5.).

---

[430] M. Chambon, *Les fichiers, nouvel instrument de police administrative ?*, dans Fichiers informatiques et sécurité publique, sous la direction de B. Plessix et N. Deffains, coll. Droit, Politique, Société, éd. PUN Universitaires de Lorraine, 2013, p. 91-108. Dans cet ouvrage, M. Chambon opère une analyse téléologique des fichiers.

[431] R. Chapus, *Droit administratif général,* Montchrestien, 15e ed., 2001, p. 737.

[432] M. Chambon cite ici les conclusions du commissaire du gouvernement Delvolvé. CE Sect., 11 mai 1951, *Consorts Baud, Rec.*, p. 265 ; S., 1952, 3, 13, concl., J. Delvolvé, note R. Drago ; TC, 7 juin 1951, *Dame Noualek, Rec.*, p. 636, concl., J. Delvolvé ; S., 1952, 3, 13, note R. Drago.

[433] M. Chambon, *Les fichiers, nouvel instrument de police administrative ?*, *op. cit.*

§1. La prévention des infractions par les fichiers à vocation judiciaire et de renseignement

147. Prévention des infractions – Les fichiers à vocation judiciaire et fichiers de renseignements ont pour but le recueil d'informations essentiellement qualitatives. Ces informations recoupées avec d'autres permettent de prévenir la commission d'infractions. De par cette même finalité générale de prévention, les deux catégories sont abordées au sein d'une même partie. Cette vocation préventive relève par nature des fichiers de renseignement mais les évoluions démontrent à la fois un rôle de prévention de plus en plus affirmé au sein de fichiers judiciaires et un rapprochement entre polices administrative et judiciaire. Il faut donc s'intéresser aux fichiers de renseignement notamment du fait de la porosité de la frontière avec le judiciaire. Parmi les fichiers à finalité préventive on retrouve les fichiers à vocation judiciaire (A) et les fichiers de renseignement (B).

A. Les fichiers à vocation judiciaire

148. Présentation – Dans la catégorie des fichiers à vocation judiciaire, on trouve par exemple le fichier des véhicules volés[434], le fichier des objets signalés[435] (qui ont fusionné avec la création du fichier des objets et véhicules signalés en 2009) ou le fichier national du faux monnayage[436]. Ces différents fichiers contiennent des informations et indications précises sur des faits, objets ou procédures dans un domaine précis et permettant leur identification ou suivi. On peut également citer le système d'information Schengen (SIS) créé par la convention d'application de l'Accord Schengen du 19 juin 1990. S'agissant d'un fichier commun à tous les Etats membres de l'espace Schengen permettant la centralisation des données, ce fichier sera abordé dans le second chapitre relatif au partage de données fichées[437].

L'idée n'est pas d'établir une présentation exhaustive de tous les fichiers, mais de s'intéresser à ceux présentant le plus d'interrogations quant au sujet du traitement des données personnelles. C'est le cas notamment du répertoire des données à caractère personnel

[434] Fichier des véhicules volés, arrêté du 15 mai 1996.
[435] Fichier des objets signalés.
[436] Fichier national du faux monnayage (FNFM), issu des principes posés par la Convention de Genève de 1929 et répondant aux obligations européennes définies dans le règlement européen 1338-2001 du 28 juin 2001, mis en service au moment de la mise en circulation de la monnaie unique au 1er janvier 2002.
[437] V. *infra* n°238 s.

collectées dans le cadre de procédure judiciaires (REDEX) (1°), et de la plateforme nationale des interceptions judiciaires (PNIJ) (2°).

1° Le répertoire des données à caractère personnel collectées dans le cadre de procédures judiciaires (REDEX)

149. Répertoire des données à caractère personnel collectées dans le cadre de procédures judiciaires – Le répertoire des données à caractère personnel collectées dans le cadre de procédures judiciaires (REDEX), a été créé par la loi du 10 mars 2010[438]. Après délibération de la CNIL le 16 juin 2016[439], le décret d'application a été adopté le 7 octobre 2016[440]. Le dispositif est entré en vigueur le 1er mars 2018 et a fait l'objet d'une circulaire en date du 11 avril 2018[441]. Placé sous l'autorité du ministre de la justice et tenu par le service du casier judiciaire, ce fichier est destiné à centraliser toutes les expertises et examens psychologiques et psychiatriques réalisés à l'encontre d'une personne poursuivie ou condamnée lorsqu'un suivi socio-judiciaire est encouru. Le but est de faciliter l'accès aux données relatives à la personnalité des individus et l'évaluation de leur dangerosité, favorisant ainsi la prise de décision et l'individualisation des peines. Sont enregistrées dans ce fichier toutes les expertises réalisées du stade de l'enquête à l'exécution éventuelle de la peine. Il contient des informations relatives à la personne et son identité, le cadre dans lequel l'examen a été ordonné, l'autorité ayant ordonnée la mesure, la nature et la date de l'infraction pour laquelle la personne est poursuivie ou condamnée. Ces données sont conservées trente ans à compter de la date de réalisation de l'expertise.

Codifié aux articles 706-56-2 et R53-21-1 à R53-21-25 du code de procédure pénale, ce fichier a vocation à n'être accessible que par les autorités judiciaires. Ce dernier a, avant même son entrée en vigueur, soulevé de vives interrogations notamment concernant la nature des données concernées puisqu'il s'agit notamment de conserver des données médicales. La seconde interrogation porte sur le fichage des données concernant des personnes simplement poursuivies et non condamnées et les atteintes éventuelles en termes de présomption d'innocence.

[438] Loi n°2010-242 du 10 mars 2010 tendant à amoindrir le risque de récidive criminelle et portant diverses dispositions de procédure pénale, codifié à l'article 706-56-2 du code de procédure pénale.
[439] Délibérations n°2016-181 du 16 juin 2016.
[440] Décret n°2016-1338 du 7 octobre 2016.
[441] Circulaire, CRIM/2018-5/Q-11.04.2018, du 11 avril 2018.

150. Interrogations quant à la nature des données enregistrées – Le répertoire REDEX vise la collecte et l'enregistrement des données d'expertises et examens, psychiatriques ou médico –psychologiques réalisés au cours d'une enquête, d'une instruction, d'un jugement, de l'exécution d'une peine, avant une mesure de rétention de sureté, ou lorsqu'est prononcé un arrêt ou un jugement en irresponsabilité pour cause de trouble mental[442]. Le premier constat est celui de la multitude des procédures pouvant aboutir à l'enregistrement des données d'expertise au sein du répertoire REDEX puisque la loi vise grand nombre d'entre elles, de l'enquête à l'exécution de la peine. Le fichier a donc vocation à contenir, outre les données permettant l'identification de la personne concernée et celle de l'autorité ayant ordonnée l'expertise, des données relatives à la procédure pénale dans le cadre de laquelle la mesure a été ordonnée, et des données médicales telles que visées par l'article 6 de la loi informatique et libertés et donc des données dites sensibles. La circulaire précise que le répertoire REDEX conserve en fichiers informatiques au format PDF les rapports d'expertise qui ont fait l'objet d'une discussion contradictoire au cours de la procédure[443]. Toutes les données médicales contenues dans l'expertise sont donc enregistrées au sein du REDEX. Dans sa délibération du 16 juin 2016, la CNIL avait appelé à la vigilance tant du fait du volume de données concernées par le traitement que du caractère sensible de celles-ci. Au vu des menaces pesant sur la vie privée des individus, la commission rappelait que des garanties suffisantes devaient être prévues et notait qu'en ce sens, le législateur plaçait le fichier sous le contrôle d'un magistrat. De plus, la commission prend note que le législateur réserve l'accès au fichier à l'autorité judiciaire ce qui constitue une seconde garantie. Plus précisément, ne peuvent accéder aux données du REDEX que les autorités judiciaires et les experts désignés par celles-ci[444].

151. Interrogations quant au profil des personnes visées par le fichage – Une des interrogations soulevées lors de la mise en œuvre du REDEX portait sur le profil des personnes visées par un potentiel fichage. Si l'enregistrement suppose la commission d'une infraction pour laquelle un suivi socio-judiciaire est encouru[445], cet enregistrement peut intervenir dès le stade de l'enquête. En cas de classement sans suite, non-lieu, relaxe ou

[442] Art. 706-56-2 du code de procédure pénale.
[443] La circulaire précise à ce sujet que les examens psychologiques réalisés au cours d'une garde à vue et qui n'ont pas été notifiés à la personne concernée ne peuvent donc pas être enregistrés au fichier REDEX.
[444] Art. 706-56-2 du code de procédure pénale.
[445] *Ibid.*

acquittement, les données sont immédiatement effacées[446]. Ainsi, lorsque cela se présente, le procureur de la République doit « dans les meilleurs délais » enregistrer une demande d'effacement. Le service gestionnaire traite ensuite la demande « dans les plus bref délais ». Afin d'apporter une meilleure garantie à ce sujet, est prévu un dispositif d'alerte sur le logiciel de chaine pénale (CASSIOPEE) utilisé dans les juridictions afin que l'utilisateur soit informé de la nécessité d'effacer une fiche au REDEX. Concrètement, lorsqu'un classement sans suite ou une relaxe est saisie sur CASSIOPEE, une alerte automatique informe qu'une fiche REDEX doit être supprimée. Il s'agit donc là d'un rapprochement entre le logiciel de chaine pénale et le REDEX permettant une meilleure mise à jour des données. Dans tous les autres cas, il appartient à l'intéressé de demander l'effacement des données au REDEX. La CNIL a soulevé la question de l'effacement des données suite à l'annulation d'une condamnation. Cette hypothèse nécessite qu'une demande d'effacement soit déposée par l'intéressé. La commission avait considéré dans son avis que dans ce cas précis, l'effacement devrait être automatique comme c'est le cas pour le casier judiciaire national. Cette suggestion n'a néanmoins pas été suivie d'effets. Afin d'éviter tout doublon ou erreur lors de la saisie de fiches au REDEX, il est prévu qu'une vérification de l'identité soit réalisée par le gestionnaire à partir du répertoire national d'identification des personnes physiques (RNIPP). Ce dispositif avait été suggéré par la CNIL et le décret d'application est venu modifier les dispositions du code de procédure pénale[447] afin de rendre possible ces vérifications.

2° La plateforme nationale des interceptions judiciaires (PNIJ)

152. Plateforme nationale des interceptions judiciaires – La plateforme nationale des interceptions judiciaires (PNIJ) centralise toutes les écoutes judiciaires ordonnées au cours d'enquêtes ou d'instructions préparatoires et les données de connexion. Créé par un décret du 9 octobre 2014[448], la loi du 3 juin 2016[449] modifiée par celle du 28 février 2017[450] est venue encadrer ce fichier automatisé. Ce dispositif a été mis en place en réponse au développement des télécommunications. Il apparaissait en effet nécessaire de revoir le cadre légal et matériel des interceptions. La plateforme est placée sous la responsabilité du secrétaire général du ministère de la justice. Elle permet de stocker les données issues d'interceptions telles que des

[446] *Ibid*.
[447] Art. R64 du code de procédure pénale.
[448] Décret n°2014-1162 du 9 octobre 2014.
[449] Loi n°2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale.
[450] Loi n°2017-258 du 28 février 2017 relative à la sécurité publique.

conversations téléphoniques, des messages, des courriels, des données de connexion et géolocalisation en temps réel[451]. En raison de la complexité de mise en œuvre, l'entrée en vigueur du dispositif a été reportée à plusieurs reprises et le dispositif lui-même ne cesse d'être repensé en vue de son amélioration. Le but annoncé était celui d'une simplification dans l'accès aux interceptions en donnant un accès direct aux magistrats[452]. Aussi, la plateforme permet une mise sous scellés numérique des données. Les données sont alors conservées tant que l'action publique n'est pas prescrite. Visant à faciliter la procédure, les réquisitions relatives aux interceptions se font directement via la plateforme en application des dispositions de l'article 230-45 du code de procédure pénale. Néanmoins, ce nouveau dispositif ne cesse de diviser[453].

153. Des interrogations quant à la nature des données visées – La plateforme centralise diverses données fixées à l'article R40-46 du code de procédure pénale. Ces données sont recueillies dans le cadre d'interceptions ordonnées par le juge d'instruction[454], et dans le cadre d'une réquisition judicaire notamment[455]. Ainsi, outre les données portant sur l'identité de la personne, elle vise les communications téléphoniques (appels, sms, msm, mails), les données de connexion (fadettes, numéros entrants et sortants, localisation de l'appareil en temps réel et traçage des relais d'émission). Ce faisant, la plateforme est susceptible de centraliser grand nombre de données à caractère personnel soulevant pour certaines davantage d'interrogations. C'est le cas notamment des données qui peuvent être enregistrées et qui entrent dans le champ de l'article 6 de la loi informatique et libertés, comme les données relatives aux opinions politiques ou convictions religieuses. Aucune disposition particulière n'est prévue s'agissant du traitement de ces données[456]. Aussi, la plateforme permet l'enregistrement et la conservation de données de reconnaissance vocale durant toute la procédure ce qui a pu être

[451] Art. R40-46 du code de procédure pénale.
[452] Auparavant, les magistrats avaient seulement accès aux écoutes par le biais des procès-verbaux qui étaient dressés par les officiers de police judiciaire en charge des mesures.
[453] Il lui est reproché notamment son coût. Voir à ce sujet le rapport de la Cour des comptes du 18 février 2016 (S2016-0336-1). Le rapport fait état d'un coût de 122,55 M €. Aussi, des interrogations sont soulevées s'agissant des potentielles atteintes aux libertés fondamentales de par tout d'abord l'étendue du type de données visées par les interceptions (sms, appels, mms, données de connexion…). D'autre part, les craintes portent sur la nature des données visées à savoir que peuvent être interceptées des données relatives aux opinions politiques et aux convictions religieuses par exemple tel qu'en dispose l'article R40-44 du code de procédure pénale. Voir à ce sujet, G. Thierry, Comment le ministère de la justice espère rebondir sur le dossier des écoutes judiciaires, *Dalloz actualité*, 21 novembre 2018.
[454] Art. 100 à 100-7 du code de procédure pénale.
[455] Art. 60-2, 77-1-2 et 99-4 du code de procédure pénale.
[456] C. Serre, C. Evrard, Du rififi chez les grandes oreilles, Etude sur les enjeux des interceptions judiciaires dans la procédure pénale au prisme de la plateforme nationale des interceptions judiciaires, *Dalloz Actualité*, 4 février 2020.

présenté par certains comme un entérinement du recours à l'authentification comme élément de preuve[457]. La CNIL appelée à rendre un avis sur le projet de décret autorisant la mise en œuvre de la plateforme a considéré s'agissant de la nature des données concernées que les données collectées sont adéquates, pertinentes et non excessives au vu de la finalité du traitement[458].

154. Une difficile conciliation avec les droits fondamentaux et libertés individuelles – De par la nature des données stockées sur la plateforme des interceptions judiciaires, se posent des interrogations en termes de droits fondamentaux. La Cour européenne des droits de l'homme admet depuis longtemps que les conversations téléphoniques et les correspondances entrent dans le champ d'application de l'article 8 de la convention européenne[459]. Le recours à des moyens de recueil de données tels que la captation, la sonorisation ou la géolocalisation soulève des interrogations en termes de droits fondamentaux. Ces interrogations sont renforcées lorsqu'il est question de stocker ces données au sein d'une plateforme nationale. Au vu des arrêts prononcés en matière de captation de conversations, il ne fait nul doute que le recours à la plateforme constitue une ingérence dans le droit au respect de la vie privée.

B. Les fichiers de renseignement

155. Le renseignement au service de judiciaire – Les fichiers de renseignement ou fichiers « d'intérêt criminel[460]», bien qu'utilisés par les services de renseignement peuvent parfois l'être par les autorités judiciaires, ce qui justifie une étude de ces derniers. Ces fichiers contiennent des informations « remarquables[461] ». L'erreur serait de croire que ces fichiers ont exclusivement un rôle en matière de sécurité nationale. Le développement de certaines formes de criminalité (notamment du terrorisme) tend à rendre la frontière entre fichiers administratifs et fichiers de police de plus en plus poreuse. Le renseignement général est désormais en lien étroit avec le système judiciaire. Le renseignement a un rôle « d'anticipation[462] », il s'agit d'un nouvel outil de prévention et de répression.

[457] *Ibid.*
[458] Délibération n° 2014-009 du 16 janvier 2014 portant avis sur un projet de décret autorisant la mise en œuvre d'un traitement automatisé de données à caractère personnel dénommé « Plate-forme nationale des interceptions judiciaires ».
[459] Cour E.D.H., 2 aout 1984, *Malone c/ Royaume-Uni*, req. 8691/79, §64. Cour E.D.H., 24 avril 1990, *Kruslin c/ France*, req. 11801/85, §25. Cour E.D.H., 24 avril 1990, *Epoux Huvig c/ France*, req. 11105/84 § 26.
[460] A ce sujet voir, F. Farcy, JF. Gayraud, *Le renseignement criminel*, CNRS éditions, Biblis, 2011.
[461] F. Farcy, JF. Gayraud, *Le renseignement criminel, op. cit.*, p. 28.
[462] *Ibid.* p. 40.

156. Les fichiers des services de renseignement – Parmi les fichiers à vocation informative et de renseignement, il convient de citer les fichiers communément qualifiés de « fichier de renseignement » en référence au service de renseignement assurant leur gestion et leur alimentation. Autrefois désignés comme les services du renseignement général, ces fichiers sont désormais gérés par la Direction générale de sécurité intérieure (DGSI)[463] elle même placée sous l'autorité du ministère de l'intérieur. Le décret du 30 avril 2014 créant la DGSI dispose dans son article 1er que *« la direction générale de la sécurité intérieure est un service actif de la police nationale. Elle est chargée, sur l'ensemble du territoire de la République, de rechercher, de centraliser et d'exploiter le renseignement intéressant la sécurité nationale ou les intérêts fondamentaux de la Nation »*. Finalement, la DGSI est à la fois un service de renseignement de sécurité et un service de police judiciaire spécialisé[464]. Les renseignements collectés par les services du renseignement font l'objet d'un enregistrement au sein de différents fichiers. Ces fichiers sont sortis de la « clandestinité »[465] avec le décret n°91-1052 du 14 octobre 1991[466] qui pour la première fois fait publiquement état de l'existence de tel fichiers.

157. La base de données de sécurité publique (BDSP) et le traitement de données à caractère personnel relatif à la gestion de l'information et la prévention des atteintes à la sécurité publique (GIPASP) – La base de données de sécurité publique (BDSP) est venue remplacer l'ancien fichier « FAR » supprimé en mars 2011[467]. Cette base de données est alimentée quotidiennement par les services de gendarmerie dans le cadre de leurs missions. Cette nouvelle base de données est composée de quatre modules dont le module de gestion de l'information et prévention des atteintes à la sécurité publique (GIPASP) intéressant plus

[463] La direction générale de sécurité intérieure a été créée par le décret n°2014-445 du 30 avril 2014 relatif aux missions et à l'organisation de la DGSI. Elle reprend les missions de la direction centrale du renseignement intérieur créée le 1er juillet 2008 qui avait elle même été créée par la fusion de la direction centrale des renseignements généraux (1907) et de la direction de la surveillance du territoire (1944).

[464] De par cette double fonction, les missions de la DGSI sont multiples. Elle intervient notamment en matière de contre-espionnage, de lutte contre le terrorisme, de protection du patrimoine économique et de police judiciaire spécialisée.

[465] N. Ach, « Fichiers, sécurité, libertés : quelle conciliation ? », *in* B. Plessix, N. Deffains (dir.), *Fichiers informatiques et sécurité publique,* Presse universitaire de Lorraine, « Droit, politique, société », 2013, p.25.

[466] Décret n°91-1052 du 14 octobre 1991 relatif au fichier informatisé du terrorisme mis en œuvre par les services des renseignements généraux du ministère de l'intérieur.

[467] Le Fichier alphabétique de renseignements de la gendarmerie nationale (FAR) est un des premiers fichiers de renseignement à être sorti de l'ombre. Il a été créé par arrêté du 17 septembre 1992. Il avait fait l'objet d'une déclaration à la CNIL en 1993[467]. Il se présentait sous forme de fiches nominatives manuscrites tenues par les militaires. Il ressort du rapport d'information de l'Assemblée nationale n°1548 de D. Batho et J.A. Bénisti que le fichier comportait 60 millions de fiches. Ces fiches comportaient toute sorte d'informations relatives à l'individu et permettant notamment d'appréhender sa dangerosité. Face à la difficulté de gérer ce fichier et aux contraintes légales, ce fichier a été supprimé à la fin de l'année 2010.

particulièrement le sujet des données à caractère personnel intervenant dans le cadre de procédures judiciaires[468]. Le dispositif a été institué, sur le modèle du traitement de prévention des atteintes à la sécurité publique (PASP) de la police nationale[469], par décret du 29 mars 2011[470] et codifié aux articles R.236-21 à R.236-30 du code de la sécurité intérieure. Il a vocation à recueillir, conserver et analyser les informations qui concernent les personnes « dont l'activité individuelle ou collective indique qu'elles peuvent porter atteinte à la sécurité publique »[471]. Un décret du 2 décembre 2020[472] est venu étendre le champ d'application du fichier précisant désormais sa finalité en termes de « sûreté de l'Etat »[473]. En matière de sûreté de l'Etat, le décret vise les données relatives aux « activités susceptibles de porter atteinte aux intérêts fondamentaux de la Nation ou de constituer une menace terroriste »[474].

Le second alinéa de l'article R236-21 du code de la sécurité intérieure précise que le fichier a particulièrement vocation à lutter contre le terrorisme et les violences collectives[475].

La CNIL saisie pour avis sur le projet de décret instituant le fichier avait rappelé que la « sécurité publique » est un élément de l'ordre public[476]. Le fichier comporte des données relatives au motif d'enregistrement et à l'identification de l'individu concerné notamment son état civil, sa profession, son adresse ou son numéro de téléphone ainsi que des photographies et un descriptif physique. Aussi, sont enregistrées des données relatives à son patrimoine, ses déplacements, ses activités publiques et toutes activités susceptibles de constituer une infraction ou encore l'identité des personnes avec lesquelles elle est ou a été en relation. S'agissant de la nature des données enregistrées dans le fichier, la CNIL avait préconisé dans son premier avis que ces dernières soient précisées notamment en ce qui concerne les données portant sur les activités publiques. De manière générale, dans son avis initial, la CNIL avait considéré que la finalité du traitement était respectée au vu des données stockées dans le

---

[468] Les trois autres modules sont le module « Gestion des sollicitations », « Sécurisation des interventions et demandes particulières de protection », « Gestion des événements d'ampleur ».

[469] V. *supra* n°157.

[470] Décret n°2011-340 du 29 mars 2011 portant création d'un traitement de données à caractère personnel relatif à la gestion de l'information et la prévention des atteintes à la sécurité publique.

[471] Art. R.236-21 du code de la sécurité intérieure.

[472] Décret n° 2020-1512 du 2 décembre 2020 modifiant les dispositions du code de la sécurité intérieure relatives au traitement de données à caractère personnel dénommé « Gestion de l'information et prévention des atteintes à la sécurité publique ». M. Biondo, E. Daoud, Renseignement territorial et fichage un nouveau tour de vis sécuritaire, *AJ Pénal*, 2020, 548. M. C. De Montecler, Controverse sur l'élargissement des finalités de trois fichiers de police, *AJDA*, 2020, 2398.

[473] Décret n° 2020-1512 du 2 décembre 2020.

[474] *Ibid*.

[475] La vocation de lutte contre le terrorisme a été précisée suite à l'adoption du décret 2017-1216 du 2 aout 2017.

[476] Délibération n° 2010-456 du 9 décembre 2010 portant avis sur un projet de décret en Conseil d'Etat autorisant la création du traitement de données à caractère personnel relatif à la gestion de l'information et la prévention des atteintes à la sécurité publique.

fichier et que les garanties relatives au traitement de données sensibles semblaient suffisantes[477]. Par dérogation était autorisé l'enregistrement de données portant sur les opinions politiques ou les croyances[478], le législateur ayant précisé l'interdiction d'opérer dans le fichier une sélection d'une catégorie de personne à partir d'une donnée sensible.

Toutefois, le décret du 2 décembre 2020 est venu très largement étendre la liste des données collectées dans le fichier. Désormais, ce dernier contient des données sensibles telles que des données relatives à la santé, aux opinions politiques, aux convictions religieuses ou aux habitudes de vie faisant de la dérogation le principe.

Un décret du 2 août 2017[479] est venu étendre l'accès au fichier. Ainsi, peuvent accéder aux données fichées « dans la limite du besoin d'en connaitre » les agents de la gendarmerie spécialement désignés et habilités. Dans le cadre d'enquêtes administratives peuvent être destinataires des mêmes données les agents du service national des enquêtes administratives de sécurité[480] ou du commandement spécialisé pour la sécurité nucléaire[481]. Aussi, sur demande expresse les données peuvent être transmises à tout agent de gendarmerie ou de police nationale[482]. L'identité des personnes ayant eu accès aux données est conservée et la CNIL opère un contrôle par le biais notamment d'un rapport d'activité qui lui est remis chaque année. Un rapport a été publié concernant les mineurs d'au moins 13 ans qui peuvent faire l'objet d'un fichage au GIPASP. L'analyse portait sur l'année 2017. Il ressort de ce dernier que 72,03% (soit 103) des mineurs enregistrés au fichier l'ont été pour motif de radicalisation et 12,59% (18) pour violences urbaines. Ces deux motifs constituent les principales causes d'enregistrement[483].

L'extension du fichier par le décret du 2 décembre 2020 semble avoir soulevé des réserves de la part de la CNIL qui relève le caractère top large de certaines catégories de données visées et

---

[477] Rappelant à l'époque le caractère dérogatoire de l'enregistrement de données sensibles au GIPASP et l'interdiction d'enregistrer des données médicales ou portant sur la vie sexuelle. La Commission a rappelé que s'agissant des données relatives à l'origine géographique, ces dernières ne peuvent être utilisées qu'en tant que données « factuelle et objective » reprenant ainsi la jurisprudence du Conseil constitutionnel, DC n°2007-557 du 15 novembre 2007.
S'agissant de l'accès aux données du fichier, la CNIL a soulevé quelques réserves considérant que ce dernier était trop large au vu du nombre d'agents concernés. La Commission met en avant le motif de sécurité des données et le manque de justification du « besoin d'en connaitre » de certains agents.

[478] Art. R.236-23 du code de la sécurité intérieure.

[479] Décret n°2017-1216 du 2 aout 2017 modifiant les traitements automatisés de données à caractère personnel prévus aux articles R.236-1, R.236-11 et R.236-21 du code de la sécurité intérieure.

[480] Décret n°2017-668 du 27 avril 2017

[481] Décret n°2017-588 du 20 avril 2017

[482] Art. R.236-26 du code de la sécurité intérieure.

[483] J. Richard, Rapport public du référent national, *Traitement de données à caractère personnel « Gestion de l'information et de la prévention des atteintes à la sécurité publique » de la Gendarmerie nationale en ce qu'il concerne les mineurs*, mai 2018.

la complexité attachée à ce nouveau fichier qui se veut désormais « mixte »[484]. Aussi, la Commission soulève le flou entourant la possibilité de collecter et conserver des données issues de réseaux sociaux.

Alarmant tant sur les données qui pourront être conservées que sur les éventuelles interconnexions ou rapprochements avec d'autres fichiers, il est fort à parier que le Conseil d'Etat sera saisi sur le nouveau dispositif. En effet, ce fichier mixte[485] interroge tant sur la qualité et la quantité des données visées ainsi que sur leur accès ou le droit des personnes visées. Par exemple une question se pose s'agissant du droit d'accès au fichier, celui-ci étant direct en matière de fichiers de police et indirect pour les fichiers relatifs à la sureté de l'Etat. Certaines zones d'ombre devront donc être éclaircies[486].

158. Le fichier de centralisation du renseignement intérieur pour la sécurité du territoire et les intérêts nationaux : CRISTINA – Le fichier de centralisation du renseignement intérieur pour la sécurité du territoire et les intérêts nationaux (CRISTINA) a été créé dans le courant de l'année 2008 à la suite de la fusion entre les Renseignements généraux et la Direction de la surveillance du territoire[487]. Ce dernier est soumis au *secret défense* et un décret du 27 juin 2008 est venu le dispenser de publication[488]. Il s'agit d'un fichier de souveraineté tel que défini par la loi informatique et libertés du 6 janvier 1978. Ce dernier n'a donc pas été soumis au contrôle de la CNIL. Le fichier est placé sous l'autorité de la direction centrale du renseignement intérieur. S'agissant d'un fichier dont la finalité repose dans la sûreté de l'Etat, il n'est pas soumis à des durées de conservation limitées des données et ces dernières sont accessibles uniquement par les agents habilités par le directeur des services de renseignement.

Le fichier CRISTINA doit permettre aux services de renseignement de collecter des informations utiles à l'exercice de leurs fonctions de lutte contre l'espionnage, de lutte contre le terrorisme ou de protection du patrimoine par exemple. Toutefois, il est très difficile d'obtenir des informations précises quant au type de données qui sont collectées et stockées dans ce fichier puisqu'il s'agit de données soumises au secret défense. Dans une délibération

[484] Délibération CNIL n° 2020-065 du 25 juin 2020.
[485] Renvoyant la fois au titre III et au titre IV de la loi informatique et libertés.
[486] Le constat est le même s'agissant du fichier PASP qui a connu la même évolution avec le décret 2020-1511 du 2 décembre 2020 pour lequel la CNIL a émis les mêmes réserves dans sa délibération 2020-064 du 25 juin 2020.
[487] Restructuration issue du décret n°2008-631 du 27 juin 2008.
[488] Décret n°2008-631 du 27 juin 2008 portant modification du décret n° 91-1051 du 14 octobre 1991 relatif aux fichiers gérés par les services des renseignements généraux et du décret n° 2007-914 du 15 mai 2007 pris pour l'application du I de l'article 30 de la loi n° 78-17 du 6 janvier 1978.

en date du 16 juin 2008, la CNIL a néanmoins rendu un avis favorable avec réserves au projet de décret[489]. Le fichier a fait l'objet d'un contrôle de légalité riche d'enseignements. Saisi par un collectif d'associations, le Conseil d'Etat a eu à se prononcer sur la légalité du fichier dont le décret d'application n'était pas publié. Au-delà de la question de légalité, s'est posée celle de l'accès aux données litigieuses et au respect du contradictoire[490].

159. Fichiers de renseignement source de données judiciaires – Que se soit par le jeu d'échanges de données, d'accès partagés ou par application des dispositions de l'article 40 du code de procédure pénale notamment, la porosité entre judiciaire et renseignement semble évidente, une procédure judiciaire peut trouver sa source dans une enquête des services de renseignement et amène à ne pas totalement exclure les fichiers de renseignement de cette étude[491].

Les fichiers judiciaires au-delà de la conservation des données relatives aux auteurs trouvent aussi une finalité dans la constatation d'infraction et le recueil de preuves.

§2. La constatation d'infractions et le recueil de preuves facilités par les fichiers d'antécédents judiciaires

160. Origines des fichiers de constations des infractions – L'une des principales vocations des fichiers de police est de faciliter la constatation des infractions et le recueil de preuves. Il s'agit dans un premier temps de s'intéresser à l'historique du système de traitement des infractions constatées (STIC) et du système judiciaire de documentation et d'exploitation (JUDEX) (A) afin de comprendre les motivations ayant entrainé leur fusion par la création du traitement des antécédents judiciaires (TAJ) (B).

[489] Délibération n°2008-177 du 16 juin 2008 portant avis sur un projet de décret en Conseil d'Etat portant création au profit de la direction centrale du renseignement intérieur d'un automatisé de données à caractère personnel dénommé « CRISTINA ». La délibération comme le décret n'ont pas été publiés en raison du caractère de secret défense des données qu'il contient.
[490] V. *infra* n° 341 s.
[491] V. *supra* n° 58.

A. Historique de la création du STIC et du JUDEX

161. Le système de traitement des infractions constatées (STIC) – Le système de traitement des infractions constatées (STIC) a été créé par décret du 5 juillet 2001[492]. Il fait suite au plan « Joxe »[493] de 1985 pour la modernisation de la police nationale. Le STIC était placé sous l'autorité de la direction générale de la police nationale (DGPN) et sous le contrôle du procureur de la République territorialement compétent.

L'idée était de créer un outil visant à simplifier les enquêtes. Cette application permettait à la fois d'exploiter les informations issues des procédures, de mieux gérer la documentation et également d'établir des statistiques. Le fichier comportait des informations relatives tant aux procédures judiciaires, aux infractions commises et à leurs circonstances, qu'aux personnes mises en cause ou victimes. Au 1er octobre 2012, le STIC comptait 45 966 390 procédures enregistrées, 6 732 561 fiches de mis en cause. 98 198 agents étaient habilités à consulter le fichier[494].

Le STIC contenait des informations relatives aux enquêtes telles que le lieu de commission de l'infraction, la date, le mode opératoire utilisé ainsi que les objets éventuels ayant eu un rôle dans la réalisation de l'infraction. Ensuite, le fichier recensait des informations relatives aux individus mis en cause dans les enquêtes. On y retrouvait leur identité (nom, prénom, sexe), leur surnom éventuel, alias, date et lieu de naissance, la situation matrimoniale et familiale, la nationalité, l'adresse, la profession ainsi qu'un signalement et une photographie. Enfin, le fichier contenait des informations relatives aux victimes d'infractions. Étaient inscrits leur identité, date et lieu de naissance, situation familiale, nationalité, adresse, profession ainsi qu'un signalement et une photographie dans le cas de disparition ou de corps non identifié. Les conditions pour faire l'objet d'une inscription au STIC étaient l'ouverture d'une procédure pénale à l'encontre d'une personne pour laquelle des éléments graves et concordants permettent de penser légitimement qu'elle a participé à la commission d'un crime, délit ou contravention de 5ème classe[495], ou en être la victime[496].

[492] Décret n°2001-583 du 5 juillet **2001** pris pour l'application des dispositions du troisième alinéa de l'article 31 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et portant création du système de traitement des infractions constatées**,** modifié par le décret n°2006-1258 du 14 octobre 2006 ; décret n°2002-424 du 28 mars 2002 ; loi n°2003-239 du 18 mars 2003 pour la sécurité intérieure. Voir la circulaire du ministère de la Justice du 6 juillet 2001 présentant les dispositions du décret.

[493] En référence à Pierre Joxe, ministre de l'intérieur de juillet 1984 à mars 1986.

[494] Chiffres CNIL au 27 mai 2013.

[495] Contravention de 5 e classe telle que visées par le décret n°2001-583 du 5 juillet 2001.

[496] Source, CNIL.

Ce fichier était alimenté par les services de police judiciaire dans le cadre de leurs enquêtes. La durée de conservation des données dépendait de la nature de l'infraction commise ainsi que du statut de l'individu et de son âge. Plus précisément, les informations relatives au mis en cause majeur étaient conservées 20 ans. Ce délai pouvait être par exception réduit à 5 ans ou au contraire porté à 40 ans pour les infractions les plus graves[497]. Les informations relatives au mis en cause mineur étaient conservées 5 ans porté à 10 ou 20 ans par dérogation[498]. Enfin, les données concernant les victimes étaient soumises à une durée de conservation de 15 ans maximum. Toutefois, lorsque l'infraction portait sur des armes, bijoux ou œuvres d'art, le délai était prolongé jusqu'à la découverte des objets en question.

A partir d'une simple requête, le fichier était interrogé en fonction des informations fournies par la victime ou par un témoin.

Ce fichier avait pour vocation de faciliter les enquêtes en regroupant les informations recueillies lors des procédures et permettant ainsi une meilleure documentation.

162. Le système judiciaire de documentation et d'exploitation (JUDEX) – Le JUDEX a été créé par décret du 17 novembre 2006[499]. Il s'agissait d'un système d'information judiciaire de la gendarmerie nationale créé par le ministère de l'intérieur. Le JUDEX était un équivalent du STIC mais à destination de la gendarmerie. De la même manière, ce fichier visait à faciliter la constatation d'infractions, les enquêtes et la recherche des auteurs. Le JUDEX recensait des informations collectées lors d'interventions. Comme pour le STIC, le fichier contenait des données relatives aux personnes à l'encontre desquelles étaient réunis des indices graves ou concordants rendant vraisemblable leur participation à un crime, délit ou contravention de 5ème classe. Contrairement au STIC, il arrivait que dans certaines procédures les données ne soient pas enregistrées (c'est le cas par exemple en matière contraventionnelle ou lorsque les informations recueillies ne présentent pas suffisamment d'utilité). Ce fichier n'était donc pas un outil statistique. Étaient habilités à accéder à ces données, les agents de la gendarmerie et de la police judiciaire, les membres du Parquet, les magistrats instructeurs ainsi que les organismes de coopération internationale (le fichier étant d'ailleurs alimenté par les données détenues par ces organismes). Les durées de conservation des données étaient identiques à celles du STIC.

[497] La liste des infractions portant la conservation des données relatives aux mis en cause majeurs est fixée dans l'annexe I du décret du 5 juillet 2001.

[498] La liste des infractions portant la conservation des données relatives aux mis en cause mineurs est fixée dans les annexes II et III du décret du 5 juillet 2001.

[499] Décret n°2006-1411 du 17 novembre 2006. S'il acquiert son existence légale en 2006, le JUDEX a néanmoins été mis en œuvre bien plus tôt dès 1986 afin de remplacer un système devenu obsolète le MIDOS.

B. La fusion du STIC et du JUDEX portant création du TAJ

163. Fusion STIC/JUDEX – La création du traitement des antécédents judiciaires (TAJ) découle de la loi du 14 mars 2011 dite « LOPPSI II »[500] codifiée aux articles 230-6 à 230-11 du code de procédure pénale. L'objectif est de renforcer les moyens de lutte contre la criminalité. Une des mesures a été la fusion du STIC et du JUDEX par le décret du 4 mai 2012[501]. Ce décret est intervenu après avis de la CNIL du 7 juillet 2011. Concrètement, le TAJ est entré en vigueur avec son décret d'application du 4 mai 2012. Il remplace dans un premier temps le JUDEX qui a été supprimé au 31 décembre 2013 et le STIC à compter du 1er janvier 2016. La mise en œuvre du TAJ reprend les vocations des fichiers qu'il remplace et apporte de nouvelles garanties tout en soulevant de nouvelles craintes. Il convient d'observer les motivations de la fusion (1°) ainsi que les nouvelles garantes apportées (2°).

1° Les motivations de la fusion STIC / JUDEX

164. Objectif de mutualisation des données – Les motivations qui ont conduit à la création du traitement des antécédents judiciaires résident clairement dans la volonté de développer un outil permettant de faciliter la constatation et la répression des infractions pénales. En rassemblant les informations collectées par les services de police et de gendarmerie, cet outil mutualise les données et augmente l'efficacité du nouveau fichier d'antécédents.

165. Les dysfonctionnements du STIC/ JUDEX – Plusieurs contrôles réalisés par la CNIL avaient mis en exergue des dysfonctionnements concernant le fonctionnement des anciens STIC et JUDEX. Ces dysfonctionnements étaient notamment liés à un grand nombre d'erreurs de saisie constatées dans les fichiers et à une absence de mise à jour de ces derniers.
La création du TAJ et son interconnexion à CASSIOPEE devait être une réponse à ces dysfonctionnements[502].

166. Données conservées au TAJ – Ce nouveau fichier est placé sous l'autorité du ministère de l'intérieur[503]. Les informations collectées dans ce fichier sont similaires à celles que

[500] Loi LOPPSI II n°2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure 2.
[501] Décret n°2012-652 du 4 mai 2012.
[502] E. Allain, Fichiers d'antécédents : un rapport préoccupant, *AJ Pénal*, 2013, 370. M. Schwendener, *Police technique et scientifique, op. cit.*

contenaient les fichiers STIC et JUDEX qu'il remplace. Le TAJ a d'ailleurs été initialement alimenté par une reprise de données des anciens fichiers STIC et JUDEX ce qui a soulevé certaines inquiétudes.

Le nouveau fichier permet donc la collecte de données relatives aux mis en cause dans des procédures (enquêtes préliminaire, flagrance, commissions rogatoires) lorsque des indices graves ou concordants rendent vraisemblable qu'ils aient participé à la commission d'un crime, délit ou contravention de 5ème classe.

Concernant les mis en cause, le fichier recense l'identité, la situation familiale, la filiation, la nationalité, l'adresse, la date et lieu de naissance, la profession, l'état de la personne ainsi qu'un signalement et une photographie (permettant de recourir au dispositif de reconnaissance faciale). Concernant les personnes morales, les informations portent sur la raison sociale, l'enseigne commerciale, le sigle, la forme juridique, l'IRCS, le SIREN, le SIRET ainsi que le lieu du siège social et le secteur d'activité et adresse.

Le traitement des antécédents judiciaires recense également des informations relatives aux victimes. Il collecte leur identité, leur situation familiale, leur nationalité, leur adresse, leur date et lieu de naissance, leur profession. La victime personne morale fait également l'objet d'un enregistrement (raison sociale, enseigne, sigle, forme juridique, IRCS, lieu du siège social, secteur d'activité, adresse).

Sont également collectées les informations relatives aux procédures d'enquête ou d'instruction pour « recherche des causes de la mort » ou disparition[504]. Les données conservées sont selon les cas l'identité de la personne, sa situation familiale et professionnelle, son adresse, sa nationalité, ses dates et lieu de naissance, son état, son signalement (pour les personnes disparues ou pour les corps non identifiés), sa photographie. Dans ces cas précis, sont également conservées des données relatives aux faits et objet de l'enquête ainsi que des détails sur la date et le lieu de commission de l'infraction, au mode opératoire. Par exception à l'article 6 de la loi informatique et libertés, des données dites sensibles peuvent faire l'objet d'un traitement, ces données permettant l'identification de la personne.

L'inscription au TAJ est faite par les agents de la gendarmerie exerçant une mission de police judiciaire et spécialement désignés à cette fin, les agents des douanes judiciaire, les magistrats du Parquet ainsi que les agents des services judiciaires habilités par le procureur de la République.

---

[503] Ministère de l'intérieur Direction générale de la police nationale et Direction générale de la gendarmerie nationale.

[504] Procédures au sens l'article 74 et 74-1 du C.P.P.

167. Durées de conservation – Les durées de conservation des données reprennent celles qui étaient applicables au STIC et au JUDEX[505]. Toutefois, concernant les procédures édictées à l'article 74 et 74-1 du CPP, les données peuvent être conservées le temps nécessaire à l'enquête, c'est à dire jusqu'à ce que la personne disparue soit retrouvée par exemple.

168. Accès au fichier – Par principe sont autorisés à accéder aux données du TAJ les agents alimentant le fichier ainsi que les agents d'Etat investis de pouvoirs de police judiciaire, les magistrats instructeurs et les organismes de coopération internationale et dans certains cas les services de police des étrangers[506].

Dans le cadre du décret du 6 septembre 2005[507], le fichier est désormais accessible en matière d'enquête administrative.

En février 2015, 9,5 millions de personnes faisaient l'objet d'une inscription au fichier de traitement des antécédents judiciaires en tant que mises en cause[508]. En 2018, le rapport de la commission des lois relatif aux fichiers mis à la disposition des forces de sécurité fait état de 18,9 millions de personnes fichées en tant que mises en cause et plus de 87 millions d'affaires enregistrées[509].

2° Les nouvelles garanties apportées

169. Mise à jour du fichier – Le nouveau fichier de traitement des antécédents judiciaires est censé apporter de nouvelles garanties notamment concernant les questions de mise à jour. L'interconnexion avec l'application du ministère de la Justice CASSIOPEE doit permettre une mise à jour automatique de la base de données du TAJ. Cela devrait régler la question de l'absence de mise à jour en cas de classement sans suite, de relaxe, de non-lieu ou d'acquittement. CASSIOPEE étant renseigné en temps réel de l'avancée de la procédure, le

[505] Conservation de 20 ans pour les données concernant les mis en cause majeurs (réduite à 5 ans ou portée à 40 ans en fonction de la gravité des faits) ; conservation de 5 ans concernant les mis en cause mineurs (réduite à 10 ans ou portée à 20 ans en fonction de la gravité des faits) ; conservation de 15 ans concernant les données relatives aux victimes.

[506] Au sens des dispositions de l'article 24 de la loi du 18 mars 2003.

[507] Décret n°2005-1124 du 6 septembre 2005 pris pour l'application de l'article 17-1 de la loi n° 95-73 du 21 janvier 1995 et fixant la liste des enquêtes administratives donnant lieu à la consultation des traitements automatisés de données personnelles mentionnés à l'article 21 de la loi n° 2003-239 du 18 mars 2003. Le TAJ peut être consulté s'agissant des enquêtes mentionnées à l'article L. 114-1 du code de la sécurité intérieure, pour les demandes de nationalisation, ou dans le cadre de certaines enquêtes de police administrative.

[508] Source CNIL, 17 février 2015.

[509] Rapport d'information de la commission des lois constitutionnelles, de la législation et de l'administration générale de la République sur les fichiers mis à la disposition des forces de sécurité, Députés Paris D. et Morel-A-L'Huissier P., déposé le 17 octobre 2018.

fichier d'antécédents judiciaires devrait l'être également. Selon la CNIL cette interconnexion devrait répondre à l'un des principaux dysfonctionnements observés dans les fichiers STIC et JUDEX[510].

170. Contrôle plus effectif – Par ailleurs, le nouveau fichier doit être soumis à un triple contrôle ce qui devrait garantir la véracité des informations qu'il contient. Dans un premier temps les procureurs de la République ont la charge de s'assurer de l'effacement ou de la rectification des données. Ils doivent également vérifier la qualification pénale des faits enregistrés. Cette vérification de la qualification est primordiale puisque c'est en partie elle qui fixe la durée de conservation des données dans le fichier. Aussi, et tel que le prévoit la loi LOPPSI II, un magistrat référent doit être désigné et a la charge de la mise à jour des données. Enfin, la CNIL en tant qu'autorité indépendante exercera un contrôle global sur le fichier.

§3. L'identification des individus par le biais de données génétiques et biométriques

171. Fichiers d'identification – La création des fichiers dits « d'identification » a foncièrement modifié la recherche des auteurs d'infractions. De la collecte de données biométriques puis biologiques à celle de l'ADN, il apparaît évident que l'utilisation de ces fichiers a apporté des moyens d'action permettant des identifications impossibles auparavant.
Parmi ces fichiers d'identification il faut citer le fichier judiciaire des auteurs d'infractions sexuelles (FIJAIS), le fichier automatisé des empreintes digitales (FAED), le fichier national automatisé des empreintes génétiques (FNAEG), et le fichier des personnes recherchées (FPR). Bien qu'ils n'interviennent pas tous de la même manière dans les enquêtes et les procédures, une étude chronologique en fonction du type de données fichées permet de comprendre leur évolution et leur développement. Cette évolution est nécessairement liée à celle des techniques scientifiques utilisées. Cette étude chronologique permet de constater que le recours à ce type de fichiers n'est pas récent.
Ces données permettent l'identification des individus par les empreintes digitales (A), par le fichage des auteurs d'infractions (B), par l'ADN (C) ou par le fichage au sein du fichier des personnes recherchées (D).

[510] Voir, C. Féral-Schuhl, *Cyberdroit. Le droit à l'épreuve d'internet*, *op. cit.*, 133.82.

A. L'identification par les empreintes digitales

172. Empreintes digitales – L'utilisation des empreintes papillaires dans la résolution des enquêtes judiciaires est née en France sous l'impulsion de deux hommes. Alphonse Bertillon[511] qui en 1882 crée un signalement anthropométrique et Edmond Locard[512] qui est à l'origine de la création du premier laboratoire de police scientifique en 1910. Le système anthropométrique mis en place par A. Bertillon repose sur l'identification des individus par neuf mesures sur différents membres du corps humain. Cette méthode dite « Bertillonage » sera complétée par les travaux de F. Galton qui mettent en avant l'unicité des empreintes digitales de l'homme. La méthode de A. Bertillon a également permis la prise de vue, à l'échelle, des scènes de crime. Sont alors posées les bases du système d'identification judiciaire par le fichage de données anthropométriques.

En 1902, pour la première fois en France, une enquête criminelle est résolue grâce au relevé d'empreintes.[513]

Le premier fichier automatisé de police dit « d'identification » est le fichier automatisé des empreintes digitales (FAED) créé en 1987 par le décret du 8 avril[514]. Il s'agit d'un fichier commun à la gendarmerie et à la police permettant d'identifier les auteurs d'infractions en les confondant au moyen de leurs empreintes digitales. Aussi, ce fichier est utilisé afin de s'assurer de l'identité d'une personne mise en cause dans une procédure pénale ou condamnée à une peine privative de liberté. En ce sens, le fichage est aussi un moyen de lutte contre la récidive. Outre le volet répressif et préventif, le FAED est utilisé dans le cadre de recherche de personnes disparues ou d'identification de personnes retrouvées mortes et dans le cadre des vérifications d'identité en matière de rétention de personnes (mesures de rétention liée à un

[511] A. Bertillon (1852-1914), criminologue français à qui l'on doit le développement des méthodes d'anthropométrie judiciaire et notamment la création d'un signalement anthropométrique mis en œuvre sous l'influence des travaux de Francis Galton, anthropologue britannique. Ce dernier s'est lui-même inspiré des travaux du scientifique Henry Faulds à la fin du 19e siècle qui a recueilli et étudié les premières empreintes digitales ; il a soulevé leur unicité et proposé leur utilisation en matière d'identification criminelle.
La méthode de fichage anthropométrique créée par A. Bertillon consiste à recueillir les mesures telles que la taille, la hauteur du buste, la longueur et largeur de la tête, la mesure de l'oreille droite entre autre ainsi que la couleur de l'iris gauche... ce dernier considérant que ces mesures n'évoluent plus après l'âge de vingt ans.

[512] E. Locard (1877-1966), professeur de médecine légale à qui l'on doit la création du premier laboratoire d'analyses scientifiques à Lyon en 1910.

[513] Il s'agit de l'affaire dite « Dossier Scheffer » instruite par A. Bertillon. Le relevé d'empreintes a permis de confondre l'assassin.
Cette méthode fut utilisée avec succès pour la première fois en 1892 dans l'affaire « Francisca Rojas » en Argentine.

[514] Décret n°8-249 du 8 avril 1987 modifié en 2005 par le décret n°2005-585 du 27 mai 2005 qui a autorisé l'enregistrement des empreintes palmaires.

refus de se soumettre à un contrôle d'identité ou rétention administrative d'étrangers ne présentant pas les documents justifiant de leur droit au séjour)[515].

Au 1er septembre 2013, 4 682 387 personnes étaient enregistrées dans le FAED et 237 457 traces non rattachées[516]. En 2018, le fichier compte 6,2 millions de fiches et 220 000 traces non rattachées[517].

Le fichier automatisé des empreintes digitales a clairement un but en matière de recherche d'auteur d'infraction, en matière de fichage des auteurs arrêtés ou condamnés et en matière de vérification de l'identité d'une personne qui ne serait pas en mesure de la prouver.

Les empreintes sont relevées par des agents des services d'enquête et transmises en fonction des cas au service central de police judiciaire, au service de la gendarmerie ou à la préfecture de police de Paris qui ont en charge l'inscription au fichier. Concrètement, lorsque les services d'enquêtes relèvent des traces ou empreintes, ces dernières sont inscrites sur une fiche sur laquelle sont indiqués les noms et sexe de la personne (s'ils sont connus), la nature de l'affaire, la date et lieu du relevé, la date d'enregistrement, les clichés anthropométriques (pour les empreintes digitales ou palmaires). L'ensemble de ces fiches constituent le FAED.

Il existe différents niveaux d'habilitation qui permettent l'accès aux données. De manière générale, ce fichier est utilisé par les services d'identité judiciaire de la gendarmerie et de la police par des agents « individuellement habilités ».

Ce fichier est placé sous le contrôle d'un magistrat de l'ordre judiciaire et dépend de la responsabilité de la police judiciaire du ministère de l'intérieur.

Le décret n° 2015-1580 du 2 décembre 2015 est venu modifier les règles applicables concernant la durée de conservation des données. En effet, avant le 1er mars 2017, date d'entrée en vigueur de l'article 5 du décret, les empreintes digitales étaient conservées 25 ans maximum. Les traces quant à elles étaient conservées en fonction de la prescription légale (3 ans en matière de faits délictuels et 10 ans en matière de faits criminels). Désormais, la durée de conservation dépend de la gravité des faits, de la qualité de la personne concernée ainsi que du caractère national ou international de la procédure. Au vu de ces différents critères, la durée de conservation se situe entre 10 et 25 ans.

En 2008, le fichier a permis l'identification de 11 697 traces et de détecter 61 273 usurpations d'identité.[518]

---

[515] Voir sur le refus de se soumettre à un contrôle d'identité l'article 78-3 du CPP.
Sur la rétention de la personne étrangère ne présentant pas les documents l'autorisant à séjourner en France, article 611-4 du CESEDA.

[516] Chiffres délivrés par la CNIL au 20 juin 2016.

[517] Chiffres délivrés par la CNIL au 15 novembre 2018.

L'identification est aussi facilitée par le fichage des auteurs d'infractions.

B. L'identification par le fichage des auteurs d'infractions

173. Fichage des auteurs d'infractions – Certains fichiers ont pour vocation première l'identification des auteurs d'infractions. Cela prend notamment la forme d'un fichage fonction de l'infraction commise. On peut citer le fichier des auteurs d'infractions sexuelles ou violentes (1.) ou le fichier des auteurs d'infractions terroristes (2.).

1. Le fichier automatisé des auteurs d'infractions sexuelles ou violentes

174. Fichage des auteurs – L'identification par le fichage des auteurs d'infractions renvoie notamment au fichier judiciaire automatisé des auteurs d'infractions sexuelles ou violentes (FIJAIS) qui permet de mieux lutter contre la récidive. Il est largement admis que ce fichier a aussi un but de prévention des actes réitérants. Créé par la loi du 9 mars 2004 dite « Perben II »[519], le FIJAIS avait à l'origine vocation à conserver l'identité des auteurs d'infractions sexuelles commises sur des mineurs permettant ainsi de lutter contre la récidive et de faciliter l'identification des auteurs. Le FIJAIS est effectif depuis le 30 juin 2005 après concertation par un comité interministériel rassemblant le ministère de la Justice, celui de l'Intérieur et celui de la Défense. Placé sous la responsabilité du ministère de la Justice, il est géré par le service du casier judiciaire national sous le contrôle du magistrat qui le dirige. L'inscription au fichier a soulevé de nombreuses interrogations et notamment celle de la nature même de cette mesure tantôt qualifiée de « mesure de police »[520] tantôt de simple « mesure »[521] et parfois de « mesure de sureté »[522].

175. Inscription au FIJAIS – Le FIJAIS concerne les infractions visées à l'article 706-47 du code de procédure pénale[523]. L'inscription est automatique s'agissant des délits punis de cinq

---

[518] Chiffres issus du rapport Bauer de 2008, p. 45.
[519] Loi n°2004-204 du 9 mars 2004 dite « Perben II » portant adaptation de la justice aux évolutions de la criminalité. Décret n°2005-627 du 30 mai 2005 modifiant le code de procédure pénale et relatif au FIJAIS.
[520] Cons. const., n°2004-492 du 2 mars 2004.
[521] Cass., crim., 20 septembre 2006, pourvoi n°06-80.733.
[522] L. Priou-Alibert, Infraction sexuelle : consécration de l'automaticité de l'inscription au fichier, *Dalloz actualité*, 24 mars 2010.
[523] L'article 706-47 du code de procédure pénale vise, les « 1° Crimes de meurtre ou d'assassinat prévus aux articles 221-1 à 221-4 du code pénal, lorsqu'ils sont commis sur un mineur ou lorsqu'ils sont commis en état de récidive légale ; 2° Crimes de tortures ou d'actes de barbarie prévus aux articles 222-1 à 222-6 du même code et

ans d'emprisonnement. Ce caractère automatique a été à plusieurs reprises rappelé par la Cour de cassation[524]. S'agissant des délits dont la peine encourue est inférieure, la condamnation ne donne pas lieu à inscription sauf décision expresse[525]. Le fichier contient des informations relatives aux personnes condamnées, même de manière non définitive, pour une infraction sexuelle ou violente. Il recense également l'identité des individus mis en examen pour des faits similaires (et dont la mesure est assortie d'un placement sous contrôle judiciaire) ou ayant fait l'objet d'une mesure alternative aux poursuites, d'un non-lieu, d'une relaxe ou d'un acquittement pour des motifs d'absence de discernement. De la même manière, sont inscrits au FIJAIS, les individus ayant commis une infraction sexuelle ou violente et ayant été condamnés à l'étranger[526]. La chambre criminelle a précisé que tout individu condamné pour complicité dans la commission d'une infraction sexuelle ou violente peut faire l'objet d'une inscription au fichier[527].

176. Nature des données inscrites au FIJAIS – Par principe lorsqu'un individu est condamné pour des faits susceptibles d'être punis d'une peine de cinq ans d'emprisonnement, cette condamnation fait l'objet d'une inscription au fichier. Dans le cas d'infractions punies d'une peine inférieure, la condamnation n'est pas portée au fichier sauf si le procureur de la

---

crimes de violences sur un mineur de quinze ans ayant entraîné une mutilation ou une infirmité permanente prévus à l'article 222-10 dudit code ; 3° Crimes de viol prévus aux articles 222-23 à 222-26 du même code et délit prévu à l'article 222-26-1 du même code ; 4° Délits d'agressions sexuelles prévus aux articles 222-27 à 222-31-1 du même code ; 5° Délits et crimes de traite des êtres humains à l'égard d'un mineur prévus aux articles 225-4-1 à 225-4-4 du même code ; 6° Délit et crime de proxénétisme à l'égard d'un mineur prévus au 1° de l'article 225-7 et à l'article 225-7-1 du même code ; 7° Délits de recours à la prostitution d'un mineur prévus aux articles 225-12-1 et 225-12-2 du même code ; 8° Délit de corruption de mineur prévu à l'article 227-22 du même code ; 9° Délit de proposition sexuelle faite par un majeur à un mineur de quinze ans ou à une personne se présentant comme telle en utilisant un moyen de communication électronique, prévu à l'article 227-22-1 du même code ; 10° Délits de captation, d'enregistrement, de transmission, d'offre, de mise à disposition, de diffusion, d'importation ou d'exportation, d'acquisition ou de détention d'image ou de représentation pornographique d'un mineur ainsi que le délit de consultation habituelle ou en contrepartie d'un paiement d'un service de communication au public en ligne mettant à disposition une telle image ou représentation, prévus à l'article 227-23 du même code ; 11° Délits de fabrication, de transport, de diffusion ou de commerce de message violent ou pornographique susceptible d'être vu ou perçu par un mineur, prévus à l'article 227-24 du même code ; 12° Délit d'incitation d'un mineur à se soumettre à une mutilation sexuelle ou à commettre cette mutilation, prévu à l'article 227-24-1 du même code ; 13° Délits d'atteintes sexuelles prévus aux articles 227-25 à 227-27 du même code. »

[524] Art. 706-53-2 du code de procédure pénale. Sur le caractère automatique voir, Cass., crim., 16 janvier 2008, *pourvoi* n°07-82.115. Cass., crim., 10 février 2010, pourvoi n°09-87.570. Voir, L. Priou-Alibert, Infraction sexuelle : consécration de l'automaticité de l'inscription au fichier, *op. cit.*

[525] Art. 706-53-2 du code de procédure pénale.

[526] Art. 706-53-2 du code de procédure pénale.

[527] Cass. crim., 10 octobre 2007, *pourvoi* n°07-80.971.

République l'exige[528]. Le mineur de moins de 13 ans ne peut être inscrit au fichier sauf décision contraire du procureur de la République ou du juge des enfants ayant statué à son sujet. Le fichier contient des informations précises sur l'identité de l'individu, sur la nature et la date de la décision ayant justifiée l'inscription ainsi que des informations diverses telles que l'adresse, les modalités de l'obligation de justification du domicile ou l'inscription éventuelle au fichier des personnes recherchées[529]. Le fichier a clairement un but de surveillance des individus ayant commis une infraction grave. L'inscription au FIJAIS emporte l'obligation, pour la personne concernée, de justifier une fois par an de son adresse et de déclarer tout changement. En matière de crime punis d'au moins vingt ans de réclusion, la personne a l'obligation de se présenter tous les six mois en gendarmerie ou commissariat pour justifier de son adresse[530]. En cas de non respect de cette obligation, outre les sanctions pénales, une alerte est immédiatement déclenchée et une enquête pénale est ouverte. L'inscription au fichier est ordonnée par le procureur de la République ou le juge d'instruction ayant en charge l'enquête qui y fait procéder « sans délai »[531]. Les données ainsi fichées sont conservées pendant 20 ou 30 ans en fonction de la gravité des faits. Le FIJAIS a connu de nombreuses évolutions tant sur les motifs d'inscription que sur l'accès aux données. La loi du 13 décembre 2005[532] relative au traitement de la récidive a étendu l'inscription au FIJAIS aux auteurs d'infractions « violentes » (meurtres, tortures, actes de barbarie...). Suite à cette réforme, le fichier est parfois cité sous la dénomination de FIJAISV. Cette loi a très largement étendu la finalité initiale du fichier qui n'a plus vocation à confondre les seuls auteurs d'infractions sexuelles mais également ceux d'actes de violence grave. Finalement, depuis sa création en 2004, le fichier a vu sa finalité étendue augmentant considérablement le nombre de personnes fichées[533] et, de la même manière, le nombre de personnes habilitées à accéder à ces données. Début 2020, le fichier contenait environ 85000 fiches[534].

[528] Voir les dispositions de l'article 706-53-2 al. 3 du CPP.
La chambre criminelle de la Cour de cassation a eu à se prononcer sur la question dans un arrêt n°14-80.541, du 17 septembre 2014. La Cour rappelle que sont dispensés d'inscription au fichier les délits punis d'une peine inférieure à 5 ans d'emprisonnement (sauf décision contraire). Les délits punis d'une peine d'emprisonnement égale à 5 ans sont inscrits automatiquement (sauf demande de dispense motivée). Enfin les délits plus graves cités à l'article 706-47 du CPP sont inscrits automatiquement sans possibilité de dispense.
[529] Art. 706-53-2 du code de procédure pénale.
[530] Art. 706-53-5 du code de procédure pénale.
[531] Art. 703-53-3 du code de procédure pénale.
[532] Loi n°2005-1549 du 12 décembre 2005 relative au traitement de la récidive des infractions pénales.
[533] Au 30 juin 2005, 20 222 personnes étaient fichées au FIJAIS. Trois ans plus tard, elles étaient 42 127. Voir, rapport Bauer 2008, *op. cit.* p. 45 à 48.
[534] Chiffres issus d'un dossier de presse du ministère de la justice relatif à la présentation du plan d'action sur les contrôles d'honorabilité, février 2020.

177. Un large accès aux données du FIJAIS – Les données du FIJAIS sont largement accessibles par des autorités dont la liste n'a cessé de s'étendre depuis la création du fichier. Dans un premier temps, la loi du 25 février 2008[535] et le décret du 6 octobre 2008[536] ont étendu le nombre de personnes ayant accès au fichier en ouvrant ce dernier aux autorités administratives. Désormais, peuvent avoir accès aux données les autorités judiciaires, les agents des greffes spécialement habilités et les agents de police et de gendarmerie dans le cadre d'enquête portant sur des faits d'atteinte à la vie ou de séquestration par exemple[537]. L'accès par les officiers de police judiciaire a été étendu. Ces derniers peuvent avoir accès au fichier sur instruction ou autorisation du procureur de la République ou du juge d'instruction dans le cadre d'une enquête de flagrance, d'une enquête préliminaire ou d'une commission rogatoire au delà des infractions d'atteinte à la vie ou de séquestration. De plus, les préfets et administrations de l'Etat peuvent avoir accès au fichier notamment en matière de recrutement, affectation ou habilitation d'agents en contact avec des mineurs[538]. Toutefois les Administrations doivent motiver leur demande de consultation. Aussi, le fichier est désormais accessible aux maires, aux présidents d'établissements publics de coopération intercommunale, aux présidents de conseil départemental et aux présidents de conseil régional par l'intermédiaire des préfets dans le cadre des décisions relatives au recrutement ou à l'agrément de personnels dans le secteur de la petite enfance. On retrouve dans ces dispositions la volonté de protéger les mineurs par le fichage des individus ayant commis une infraction de nature sexuelle ou violente. Ce sujet a néanmoins soulevé de vives interrogations.

---

[535] Loi n°2008-174 du 25 février 2008 relative à la rétention de sûreté et à la déclaration d'irresponsabilité pénale pour cause de trouble mental.

[536] Décret n°2008-1023 du 6 octobre 2008 relatif au fichier judiciaire national automatisé des auteurs d'infractions sexuelles ou violentes et au casier judiciaire national automatisé.

[537] Art. 706-53-7 du code de procédure pénale.

[538] Tels que fixés par l'article R. 33-8-24 du CPP, à savoir *: « I.-En application des dispositions du 3° de l'article 706-53-7, peuvent directement interroger le fichier, par un système de télécommunication sécurisé, à partir de la seule identité d'une personne ayant formé une demande de recrutement, d'affectation, d'autorisation, d'agrément ou d'habilitation concernant une activité ou une profession impliquant un contact avec des mineurs ou dont l'exercice d'une telle activité ou profession doit être contrôlé :*
1° Les préfets ou les agents des préfectures spécialement habilités par eux à cette fin ;2° Les chefs de services ou agents individuellement désignés et spécialement habilités par eux à cette fin des administrations de l'Etat suivantes :a) La direction chargée de la gestion des ressources humaines du ministère chargé de l'éducation nationale et de l'enseignement supérieur ;b) Les rectorats et les inspections académiques ;c) La direction de la protection judiciaire de la jeunesse et ses directions régionales ;d) La direction de l'administration pénitentiaire et les directions interrégionales des services pénitentiaires ;e) La direction de la jeunesse et de l'éducation populaire et la direction des sports ;f) Les directions régionales de la jeunesse, des sports et de la cohésion sociale, les directions départementales de la cohésion sociale et les directions départementales interministérielles chargées de la cohésion sociale ;g) Les directions départementales du travail, de l'emploi et de la formation professionnelle (1).3° Les directeurs généraux des agences régionales de santé. II.-Les personnes mentionnées au I indiquent le motif pour lequel elles interrogent le fichier. »

178. L'interdiction de tout rapprochement ou interconnexion de données du FIJAIS avec d'autres traitements – L'article 706-53-11 du code de procédure pénale pose l'interdiction de toutes interconnexions ou rapprochement de données du FIJAIS avec d'autres fichiers. On peut à ce sujet citer un arrêté en date du 19 avril 2012[539] et une circulaire du 29 mai 2021[540] relatifs à la création d'un traitement automatisé de données en matière d'accueil collectif de mineurs. Ce texte institue le traitement SIAM qui a vocation à assurer la protection des mineurs lors d'accueil collectifs. Ce traitement soulevait la question du rapprochement avec le FIJAIS notamment et de la consultation automatique et systématique du fichier. Saisie pour avis la CNIL souligne que si l'administration interroge le FIJAIS en fonction d'une liste d'individus identifiés, les réponses ne contiennent pas l'identité mais un code ne permettant pas l'identification directe. Aussi, si après interrogation il s'avère que la personne est fichée au FIJAIS, l'information sera ensuite traitée par un référent spécifique habilité. La Commission précise que cette consultation est manuelle et que la réponse ne vient pas enrichir les données du SIAM. Par conséquent, ce traitement ne constitue pour la CNIL ni un rapprochement ni une interconnexion[541].

2. Le fichier judicaire automatisé des auteurs d'infractions terroristes

179. Le fichier judiciaire national automatisé des auteurs d'infractions terroristes (FIJAIT) – Sur un format très proche de celui du fichier judiciaire automatisé des auteurs d'infractions sexuelles (FIJAIS)[542], la loi du 24 juillet 2015[543] relative au renseignement a créé le fichier judiciaire national automatisé des auteurs d'infractions terroristes (FIJAIT). De la même manière que le FIJAIS, ce dernier est confié au service du casier judiciaire national et est placé sous l'autorité du ministère de la justice. Il a vocation à prévenir la récidive des infractions à caractère terroriste et à faciliter l'identification des auteurs. Sont enregistrées les

[539] Arrêté du 19 avril 2012 portant création d'un traitement automatisé de données à caractère personnel relatif à la gestion des accueils collectifs de mineurs à caractère éducatif dénommé « SIAM ».
[540] Circulaire n°DJEPVA/DJEPVAA3/2012/208 du 29 mai 2012 relative à la consultation systématique du fichier national automatisé des auteurs d'infractions sexuelles ou violentes dans le cadre des accueils collectifs de mineurs à caractère éducatif.
[541] Délibération CNIL n°2012-031 du 2 février 2012 portant avis sur un projet d'arrêté portant création du traitement automatisé de données à caractère personnel relatif à la gestion des accueils collectifs de mineurs à caractère éducatif dénommé SIAM.
[542] Voir, *supra* n°176 s.
[543] Loi n°2015-912 du 24 juillet 2015 relative au renseignement codifiée aux articles 706-25-3 et suivants du CPP. Décret 2015-1840 du 29 décembre 2015 modifiant le code de procédure pénale et relatif au fichier judiciaire national automatisé des auteurs d'infractions terroristes.

personnes condamnées, même non définitivement, pour une infraction de terrorisme[544] ou mise en examen pour des faits similaires.

Les modalités d'inscription dans le fichier sont les mêmes que celles du FIJAIS. Il faut toutefois noter que ne peuvent être inscrites les personnes faisant l'objet d'une fiche établie par les services de renseignement en dehors de toute procédure pénale.

L'inscription au FIJAIT entraîne nécessairement l'inscription au fichier des personnes recherchées.

Le fichier est alimenté en majorité par les officiers de police judiciaire, le casier judiciaire national ou le ministère des affaires étrangères mais peut également être à l'initiative du procureur de la République.

Les personnes inscrites doivent répondre à diverses obligations telles que la justification de leur adresse tous les 3 mois. Sont habilités à consulter ce fichier les officiers de police judiciaire dans le cadre d'enquêtes ou sur instruction du Parquet ou commission rogatoire. Certains représentants de l'Etat ont également accès aux données du FIJAIT dans le cadre de recrutement.

Les données sont conservées en principe 20 ans concernant les majeurs et 10 ans concernant les mineurs. Elles sont effacées en cas d'acquittement, non-lieu ou relaxe.

La création du FIJAIT répond aux évolutions de la criminalité constatée ces dernières années avec notamment une augmentation du nombre d'infractions terroristes, le but étant de pouvoir mieux identifier les auteurs tout en prévenant les récidives. Ce nouveau dispositif s'inscrit logiquement dans le nouvel arsenal qui entoure la loi renseignement de 2005 mais reste un fichier judiciaire placé sous l'autorité du ministère de la justice. Toutefois, les données stockées sont accessibles aux autorités judiciaires et aux services de renseignement dans leur mission de prévention du terrorisme.

C. L'identification par l'ADN

180. Fichage ADN – Après les évolutions liées au développement des méthodes d'identification anthropométriques une des grandes avancées a été celle de l'identification par l'ADN[545]. La base de données génétiques a été créée par la loi n°98-468 du 17 juin 1998[546]

[544] En référence aux articles L. 224-1 du code de la sécurité intérieure relatif à l'interdiction de sortie du territoire et 421-1 à 421-6 du code pénal.
[545] ADN ou acide désoxyribonucléique, constitue la molécule support de l'information héréditaire.
[546] Loi n°98-468 du 17 juin 1998 relative à la prévention et à la répression des infractions sexuelles ainsi qu'à la protection des mineurs et décret du 18 mai 2000.

suite à l'affaire dite « Guy Georges »[547] relative à plusieurs crimes commis entre 1991 et 1995. L'ADN ayant permis d'identifier l'auteur, il paraît évident que la création d'un fichier qui recenserait tous les ADN recueillis lors d'enquêtes et de poursuites permettrait d'identifier plus rapidement les suspects. Le fichier national automatisé des empreintes génétiques est alors créé[548].

181. Une extension progressive des infractions permettant le fichage au FNAEG – Le FNAEG a initialement vocation à recenser les ADN collectés dans le cadre d'affaires liées à des infractions de natures sexuelles. Un décret du 18 mai 2000[549] est venu par la suite instituer le service central de préservation des prélèvements biologiques chargé d'assurer la conservation centralisée des prélèvements.[550] Par la suite, le législateur est venu étendre le nombre des condamnations permettant l'inscription au fichier. En ce sens, la loi n°2001-1062 du 15 novembre 2001[551] étend les inscriptions aux profils ADN des individus condamnés pour tout crime contre les personnes. Aussi, la loi n°2003-239 du 18 mars 2003[552] va plus loin en étendant l'inscription à toute condamnation ou mise en cause dans des délits ou crimes perpétrés contre des personnes ou des biens prévus à l'article 706-55 du code de procédure pénale.

182. Un stockage de masse permettant une meilleure identification – Le FNAEG a vocation à faciliter l'identification des auteurs de crimes par l'ADN ainsi que l'identification de personnes disparues. Pour ce faire, le fichier recense et conserve toutes les traces ADN recueillies lors de procédures qu'elles soient ou non rattachées à un individu. Ce fichier est placé sous l'autorité de la direction centrale de la police judiciaire (DGPN) au ministère de l'intérieur et sous le contrôle d'un magistrat. Les données peuvent être consultées par les personnes habilitées de la DGPN et DGGN et par des agents spécialement habilités en matière de coopération internationale. Dans le cadre d'enquêtes, ces derniers peuvent interroger le

---

Voir les articles 706-54 à 706-56-1 du CPP.

[547] L'affaire Guy Georges dite « du tueur de l'est parisien » s'est déroulée au début des années 90. Plusieurs femmes seront violées puis assassinées selon les mêmes modes opératoires. L'assassin sera confondu grâce à l'ADN laissé sur les scènes de crime en 1998 alors qu'il était arrêté pour des faits d'agression. Son ADN est alors relevé. En 1998 le juge d'instruction en charge de l'affaire des viols suivis de meurtres demande à tous les laboratoires ayant collectés des ADN de comparer celui relevé sur les scènes de crime. Guy Georges est alors identifié.

[548] Pour une présentation détaillée, voir, V. Gautron, *Fichiers de police*, *op. cit.*

[549] Décret n°2000-413 du 18 mai 2000.

[550] C. Doutremepuich, *Les fichiers des empreintes génétiques en pratique judiciaire*, ed. Documentation française, 9 janvier 2007.

[551] Loi n°2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne.

[552] Loi n°2003-239 du 18 mars 2003 pour la sécurité intérieure.

fichier et comparer de nouvelles empreintes à celles déjà stockées. Cette comparaison peut ainsi permettre d'identifier la trace nouvelle ou au contraire celles déjà contenues dans le fichier et pour laquelle aucune identité n'était attribuée. Les données sont conservées quarante ans concernant les personnes condamnées définitivement, les personnes disparues ou les personnes décédées et vingt-cinq ans pour les personnes mises en cause dans une procédure.

La loi du 15 novembre 2001 prévoit des sanctions en cas de refus de se soumettre au prélèvement et la loi du 18 mars 2003 en fait un délit puni d'une peine d'emprisonnement et d'une amende. Toutefois, le refus peut être jugé légitime si l'infraction commise n'est pas prévue par l'article 706-55 du code de procédure pénale[553]. De fait, le FNAEG contient grand nombre de données génétiques. Au 31 août 2012 le fichier comportait 2 039 874 profils génétiques dont 1 641 476 profils de personnes condamnées, 398 698 profils de mis en cause et 149 097 traces non identifiées[554]. Ces chiffres étaient de 2,8 millions de profils fichés en 2018 et 480 000 traces non identifiées[555]. Il n'est pas rare que le recueil de traces permette d'identifier un individu dans un fichier. Le recueil ADN confronté alors au FNAEG peut le confondre dans plusieurs affaires en cours témoignant ainsi de la complémentarité des fichiers d'identification entre eux[556].

Sans méconnaître les avancées en termes de recherche de preuve qui ont accompagné la création du fichier, ce dernier soulève lui aussi des interrogations en termes de droits fondamentaux.

D. Le fichier des personnes recherchées

183. Historique –Le fichier des personnes recherchées (FPR) a été créé par arrêté du 15 mai 1996[557]. Il a vocation à contenir l'identité de toutes les personnes recherchées que ce soit par les services de police, de gendarmerie, des douanes, des administrations ou militaires. La

[553] Par exemple, le tribunal correctionnel de Bordeaux dans une décision du 28 octobre 2010 a relaxé un prévenu poursuivi pour refus de prélèvement dans le cadre d'une affaire de destruction de cultures OGM.

[554] Chiffres fournis par la CNIL, 13 février 2013.

[555] Chiffres fournis par la CNIL, 15 novembre 2018.

[556] Pour des exemples, voir, C. Ambroise-Castérot, Le FNAEG un outil de fichage au service des enquêtes, *Cahiers, droit sciences et technologies*, *In*, Le procès pénal à l'épreuve de la génétique, 2019.

[557] Arrêté du 15 mai 1996 relatif au fichier des personnes recherchées géré par le ministère de l'intérieur et le ministère de la défense, JORF n°115 du 18 mai 1996, p. 7488. Modifié par l'arrêté du 2 septembre 2005, JORF du 15 octobre 2005 relatif au fichier des personnes recherchées géré par le ministère de l'intérieur et le ministère de la défense. Cet arrêté visait à mettre le dispositif en conformité avec la loi n°200-516 du 15 juin 2000 renforçant la protection de la présomption d'innocence et les droits des victimes ; la loi n°2003-239 du 18 mars 2003 pour la sécurité intérieure dite loi « LSI » et la loi n°2004-204 du 9 mars 2004 portant adaptation de la justice aux évolutions de la criminalité dite loi « Perben II ».

fiche contient nécessairement l'indication de la conduite à tenir en cas de découverte de la personne.
Si le contenu du fichier est assez simple, son utilisation en fait un fichier particulier à vocation multiple. Pour cette raison, il semble opportun d'en faire une étude indépendante bien que celle-ci permet de comprendre que ce fichier est interconnecté à beaucoup d'autres.

184. Présentation générale du fichier – Le fichier des personnes recherchées contient vingt et une sous-rubriques en fonction du fondement juridique de la recherche. Ces sous-rubriques permettent de mieux appréhender la multitude de fonctions de ce dernier. Ces rubriques sont indiquées par une lettre apparaissant sur la fiche nominative comme par exemple « E » en matière de police des étrangers, « IT » pour les interdictions de sortie de territoire, « M » pour les fugues de mineurs, « V » pour les personnes évadées, « S » pour la sûreté de l'Etat, « PJ » pour la police judiciaire ou « T » pour les personnes débitrices envers le Trésor public.[558]
Les motifs conduisant à l'inscription au FPR peuvent être judiciaires (exécution de mandat, exécution des peines, contrôle judiciaire, enquêtes...), ou administratifs (droit des étrangers, législation fiscale, recherche de personnes disparues à la demande de la famille...) ou relever de motifs d'ordre public telle qu'une menace à la sécurité publique ou à la sûreté de l'Etat. Beaucoup de fiches vont d'ailleurs être alimentées par les services de la direction générale de la sûreté intérieure (DGSI). Le fichier est placé sous la responsabilité du ministère de l'intérieur. Les personnes sont inscrites par les agents de la direction générale de la police nationale ou de la gendarmerie ou par le juge aux affaires familiales depuis une circulaire du 12 septembre 2012[559].

185. L'utilisation du FPR en matière pénale et civile – En matière pénale, le fichier est utilisé pour l'exécution de mandats, de mesures de contrôle judiciaire ou l'exécution de décisions de justice par exemple. Il intervient aussi dans la matière civile comme sur ordonnance du juge aux affaires familiales ou du juge des enfants (par exemple en matière d'enlèvement international d'enfant pour éviter qu'un des parents ne quitte le territoire avec l'enfant alors même qu'il ne dispose pas de la garde ou que l'autre parent dispose d'un droit de

[558] Le fichier des personnes recherchées est divisé en 21 sous catégories : « E » police générale des étrangers, « IT » interdiction du territoire, « R » opposition à résidence en France, « TE » opposition à l'entrée en France, « AL » aliéné, « M » mineurs fugueurs, « V » évadés, « S » sûreté de l'Etat, « PJ » recherches de police judiciaire, « T » débiteurs envers le Trésor, « J » judiciaire, « X » personnes disparues, « CC » contraintes par corps, « F » recherches dans l'intérêt de la famille, « G » mesures administratives concernant les permis de conduire, « TM » oppositions à la sortie du territoire d'un mineur...
[559] Circulaire n°2012-1037 du 12 septembre 2012 relative à la mise en œuvre de l'interdiction de sortie de territoire sans l'accord des deux parents.

visite). L'enfant est alors inscrit au FPR afin que les autorités soient alertées d'une éventuelle sortie du territoire. De ce fait, le fichier peut être consulté par les autorités judiciaires, les services de police et de gendarmerie et dans certains cas les autorités administratives. Un décret du 28 mai 2010[560] a étendu l'inscription au fichier aux étrangers en situation irrégulière et aux fraudeurs au permis de conduire. Le nombre de fiches au FPR ne cesse d'augmenter. Par exemple au 1er novembre 2010 le FPR contenait 406 849 fiches[561], il en contient aujourd'hui 642000[562].

186. L'utilisation particulière en matière de terrorisme – Le fichier des personnes recherchées contient la fiche « S » à laquelle il est souvent fait référence en matière de terrorisme. La particularité de la fiche « S » est qu'elle ne résulte pas d'une décision administrative ou judiciaire mais résulte de simples soupçons existants concernant une personne. Le décret du 28 mai 2010 précise dans son article 2 8° que peuvent être inscrites au fichier *« les personnes faisant l'objet de recherches pour prévenir des menaces graves pour la sécurité publique ou la sûreté de l'Etat, dès lors que des informations ou des indices réels ont été recueillis à leur égard »*. La fiche « S » est elle-même divisée en différentes rubriques allant de « S1 » à « S14 ». Ce qu'il faut néanmoins savoir, c'est qu'à l'exception des fiches « J » et « PJ » le fichage au FPR ne peut entraîner aucune mesure coercitive à l'encontre des personnes. Les personnes faisant l'objet d'une fiche « S » ne font pas non plus l'objet d'une surveillance particulière. Cette fiche a plus un rôle d'alerte. Lors d'un contrôle d'identité, les autorités prenant connaissance du fichage de la personne peuvent recueillir un maximum d'informations la concernant. Toutefois, les données inscrites dans la fiche « S » ne sont conservées qu'un an. Il s'agit donc plus d'un outil de renseignement que de répression.

Après les fichiers d'identification, de constations des infractions ou de prévention, il convient de s'intéresser au cas particulier du casier judiciaire national.

§4. Le cas particulier du casier judiciaire national véritable mémoire judiciaire

187. Casier judiciaire – Le casier judiciaire national automatisé a été créé par la loi n°80-2 du 4 janvier 1980[563]. Souvent présenté comme une véritable « mémoire judiciaire »[564], ce

[560] Décret n°2010-569 du 28 mai 2010 relatif au fichier des personnes recherchées.
[561] Chiffres CNIL, 19 novembre 2013.
[562] Chiffres CNIL, 28 mars 2019.
[563] Loi n°80-2 du 4 janvier 1980 relative à l'automatisation du casier judiciaire, *Journal officiel*, 5 janvier 1980.

fichier recense les condamnations de chaque individu. Lors de la présentation du dispositif et de son inauguration, le Garde des sceaux Monsieur Badinter, l'avait qualifié de « mémoire douloureuse ».

188. Du marquage au fer au casier judiciaire – En réalité, le fichage des condamnations est bien plus ancien. Le code pénal de 1810 prévoyait le marquage au fer rouge[565] des individus condamnés qui constituait une sorte de mémoire judiciaire de l'individu puisque ce dernier était marqué à vie des condamnations prononcées à son encontre. En 1808 le code d'instruction criminelle crée les sommiers judiciaires. Il s'agit de fiches qui recensent les condamnations prononcées à l'encontre d'un individu dans des répertoires établis par juridiction. Le magistrat Arnould Bonneville de Marsangy va réformer ce système de sommiers. Les fiches individuelles seront alors directement transmises et regroupées en un fichier. C'est lui qui proposera en 1848 de créer un casier judiciaire. Les condamnations seraient alors enregistrées dans la juridiction du lieu de naissance de l'individu. Le Garde des sceaux Rouher instaure alors ce casier judiciaire par une circulaire du 3 novembre 1850.[566]
Le casier judiciaire devient « national » par un arrêté du 20 juillet 1994. Il est alors rattaché au service des affaires criminelles et des grâces. Il recense toutes les condamnations pénales prononcées à l'encontre des personnes physiques ou morales. Sont également inscrites certaines peines de natures administratives, civiles ou commerciales. Toutes les données sont centralisées au siège à Nantes.

189. Le fonctionnement en bulletins – Le casier judiciaire national est organisé en trois bulletins qui comportent des informations plus ou moins précises et détaillées. Les différents bulletins ne sont pas accessibles de la même manière. Le bulletin numéro 1 comporte toutes les condamnations et décisions de justice. Plus précisément, il contient les condamnations pénales, les décisions commerciales (telles que liquidation judiciaire ou faillite personnelle),

---

[564] Voir en ce sens, S. Grunvald, *Le casier judiciaire, Approches critiques et perspectives comparées*, sous la direction de V. De Greef et J. Pieret, Larcier, 2011, pp. 257-275.
[565] Le marquage au fer rouge ou flétrissure était une peine infamante utilisée dans l'ancien droit. Il s'agissait de marquer d'une lettre l'épaule des condamnés en fonction de la peine et de l'infraction commisse. Par exemple, une personne condamnée pour vol se voyait marquée d'un « V » ou « VV » s'il s'agissait d'une récidive ou encore « GAL » quand elle était envoyée aux galères. Cette mesure fut abolie par le code pénal de 1791 et rétablie en 1801. Le code pénal de 1810 la rend systématique en cas de prononcé de peines perpétuelles et de travaux forcés. Cette peine a été définitivement abolie en France par la loi du 28 avril 1832 contenant des modifications au code pénal et au code d'instruction criminelle.
[566] Le casier judiciaire créé en 1850 sera officialisé par la loi du 5 août 1899 et inscrit dans le code d'instruction criminelle en 1945. Après plusieurs évolutions, comme par exemple l'extension de l'inscription au casier des peines contraventionnelle, la casier judiciaire national automatisé voit le jour en 1982 sous l'impulsion de Robert Badinter.

certaines décisions administratives ou civiles (comme par exemple les jugements en déchéance d'autorité parentale). Le bulletin numéro 1 recense aussi les arrêtés d'expulsion, les mesures de composition pénale, les grâces, les réductions de peine, les libérations conditionnelles ou les suspensions de peine. Ce bulletin ne peut être consulté que par les magistrats et les établissements pénitentiaires. Les données sont conservées en fonction de la mesure et peine prononcée. Par exemple, une condamnation pour contravention ou une mesure de composition pénale est conservée trois ans au casier, un jugement de liquidation judiciaire est enregistré pour 5 ans au casier. Enfin, les condamnations pénales sont inscrites au casier pour 40 ans si elles ne sont pas suivies d'une nouvelle condamnation. Par principe, le décès de l'intéressé entraîne effacement du casier. Le bulletin numéro 2 comporte toutes les décisions à l'exception des décisions prises à l'encontre de mineurs, les peines contraventionnelles, les jugements en déchéance d'autorité parentale, les condamnations avec sursis[567], les mesures de composition pénale. Là aussi, la durée d'inscription est fonction de la nature de la décision. La condamnation au paiement de jour-amende est inscrite pour 3 ans, le jugement de liquidation judiciaire est mentionné au casier pendant 5 ans. La condamnation à une suspension de permis de conduire est effacée après la fin de la peine. Les peines pénales sont conservées 4 ans si elles ne sont pas suivies de nouvelles condamnations. Ce bulletin ne peut être délivré qu'à certaines administrations pour des motifs précis (par exemple concernant l'accès à certains emplois en relation avec des mineurs). Enfin, le bulletin numéro 3 est le plus restreint. Il contient uniquement les condamnations prononcées pour des motifs graves comme les condamnations pour crime ou délit supérieures à deux ans d'emprisonnement sans sursis, celles inférieures à deux ans si le tribunal l'ordonne, certaines déchéances ou incapacités, les mesures de suivi socio-judiciaire ou les peines d'interdiction d'exercer. Là aussi, le délai de quarante ans est applicable. Ce bulletin ne peut être délivré qu'à la personne concernée ou à son représentant légal[568].

190. Les évolutions du casier judiciaire national – Les rédacteurs de la loi instituant le casier judiciaire national avaient été sensibles aux effets « pervers » que pourrait avoir la création d'un tel fichier. A l'époque il était déjà question de la réinsertion des personnes condamnées. Si cette préoccupation demeure actuelle, s'est développée en parallèle une

[567] Sauf celles prononcées avec un suivi socio-judiciaire ou assorties d'une interdiction d'exercer une activité avec des mineurs. Dans ce cas, la condamnation est inscrite au bulletin numéro 2.
[568] Voir à ce sujet, C. Elek, *Le casier judiciaire*, Que sais-je ? n°2419, PUF, 1988.

« exigence de traçabilité »[569] qui s'inscrit dans un courant plus sécuritaire. Cette évolution couplée au développement du nombre de fichiers rend nécessairement le droit à l'oubli plus difficile à honorer[570]. A l'instar d'autres fichiers de police, le casier judiciaire national contient de plus en plus de mentions et est de plus en plus sollicité et accessible. Lors de sa création, le casier judiciaire avait pour vocation de permettre de mieux appréhender le passé judiciaire des individus et de prononcer une peine juste et plus adaptée. Le casier judiciaire intervient désormais en termes de sécurité. Loin des motivations qui ont conduit le législateur à adopter des lois[571] permettant une meilleure réinsertion des personnes condamnées, ces dernières sont désormais perçues comme « potentiellement réitérantes »[572]. Concernant le casier judiciaire, ce courant sécuritaire se traduit notamment par l'allongement des mentions portées au fichier. Par exemple, la loi n°2002-1138 du 9 septembre 2002[573] prévoit l'inscription au bulletin numéro 1 des mesures de composition pénale. La loi n°2008-174 du 25 février 2008[574] prévoit l'inscription aux bulletins numéro 1 et 2 des jugements déclarant l'irresponsabilité pénale d'un individu. La liste des personnes à qui peut être délivrée une copie du casier a également augmenté. Le bulletin numéro 1 ne peut être consulté que par des magistrats ou services pénitentiaires. Toutefois, l'interconnexion des casiers judiciaires européens a ouvert le casier judiciaire français aux autorités judiciaires des autres pays membres. La question se pose plus nettement concernant l'accès au bulletin numéro 2. Dans une recommandation de 1984, le conseil de l'Europe alertait sur la nécessité de limiter l'accès au casier judiciaire à des « intérêts légitimes »[575]. L'article 776 du code de procédure pénale et l'article R. 79 du même code précisent la liste des personnes habilitées à consulter le bulletin et les motifs de consultation. L'article R. 79 du code de procédure pénale prévoit que le bulletin numéro 2 peut être consulté par différentes administrations de l'Etat chargées de la police des étrangers, de l'assainissement des professions agricoles, commerciales, industrielles et artisanales, aux

[569] S. Grunvald, Le casier judiciaire : entre mémoire et oubli, quel équilibre aujourd'hui ? *In*, Le casier judiciaire. Approches critiques et perspectives comparées, *op. cit*., p. 206.
[570] V. *infra* n°
[571] Voir par exemple la loi n°70-643 du 17 juillet 1970 tendant à renforcer la garantie des droits individuels des citoyens et la loi n°75-624 du 11 juillet 1975 modifiant et complétant certaines dispositions de droit pénal. Cette dernière instaure notamment le sursis avec mise à l'épreuve qui vise la meilleure réinsertion des personnes condamnées.
[572] S. Grunvald, « Le casier judiciaire : entre mémoire et oubli, quel équilibre aujourd'hui ? » *In*, *Le casier judiciaire. Approches critiques et perspectives comparées*, *op. cit.*, p.263.
[573] Loi n°2002-1138 du 9 septembre 2002 d'orientation et de programmation pour la justice, dite loi « Perben I ».
[574] Loi n°2008-174 du 25 février 2008 relative à la rétention de sûreté et à la déclaration d'irresponsabilité pénale pour cause de trouble mental. Désormais, dans le cas où l'auteur de faits pénalement répréhensibles est reconnu comme étant irresponsable pour cause de trouble mental, il est renvoyé devant une juridiction de jugement qui statue sur les intérêts civils et peut prononcer des mesures de sûreté à son encontre. La déclaration d'irresponsabilité peut être portée au B1 et au B2. Voir article 768 10° C.P.P.
[575] Recommandation n° R(84) 10 du conseil de l'Europe sur le casier judiciaire et la réhabilitation des condamnés.

administrations publiques saisies de demandes d'autorisation ou détention d'armes, aux conseils de l'ordre des médecins, aux juges des enfants dans le cadre des procédures d'habilitations de personnes accueillant habituellement des mineurs par exemple. Cet article a souvent été réécrit et la liste n'a cessé de s'allonger. Si l'article 776 du code de procédure pénale fixe les motifs de consultation, la liste des personnes habilitées à accéder au bulletin est fixée par voie réglementaire.[576] En parallèle du développement exponentiel des fichiers de police, on constate une multiplication du nombre d'acteurs y ayant accès et donc une extension de la finalité de ces fichiers. C'est particulièrement cette question de l'application faite du principe initialement développé par la CNIL de finalité qui alerte une partie de la doctrine et la CNIL elle même.

Un autre sujet, conséquence des évolutions technologiques, alerte et soulève autant d'interrogations que de craintes. Il s'agit du développement de traitements permettant la prédictivité de la justice. Ce recours aux algorithmes en matière judiciaire connait un essor avec l'adoption du décret relatif à Datajust auquel il convient de s'intéresser afin de comprendre les enjeux réels d'un tel dispositif.

§5. Les traitements de données judiciaires au service de la prédictivité de la justice

191. Notion de prédictivité – Conséquence ou corollaire du *big data*, le sujet de la justice prédictive ne cesse de diviser. Certains y voient la fin des droits du procès et le début d'une justice déshumanisée[577], d'autres la présentent comme une évolution logique permettant des avancées positives si toutefois certaines garanties sont fixées[578]. De manière générale la justice dite « prédictive » renvoie à *« la démarche consistant à appliquer les techniques les plus récentes d'analyse automatique de données massives aux bases de jurisprudence dans le but affiché d'anticiper autant qu'il est possible l'issue du procès »*[579]. Le sujet appelle à s'interroger de manière générale sur les enjeux de la justice prédictive (A.) puis plus

[576] Cette fixation par voie réglementaire a été critiquée. Une partie de la doctrine considère qu'au vu des risques pesant sur les droits individuels la fixation des personnes pouvant consulter le bulletin numéro 2 devrait être fixée par une loi et non un règlement.
Voir en ce sens, V. De Greef, J. Pieret, *Le casier judiciaire. Approches critiques et perspectives comparées*, pp, *op. cit.*, 265-266.
[577] X. Labbée, La fin du monde, la fin du droit ou la transition juridique ?, *Dalloz* 2019, p. 78.
Voir, A. Garapon, J. Lassègue, *Justice digitale*, PUF, 2018.
[578] E. Buat-Ménard, La justice dite « prédictive » : pré requis, risques et attentes - l'expérience française, *Les cahiers de la justice*, 2019, p. 269.
T. Cassuto, La justice à l'épreuve de sa prédictibilité, *AJ Pénal*, 2017, p. 334.
[579] *Ibid*. Il s'agirait de ce point de vue de probabilités plus que de prédictions.

précisément sur la création de « DataJust » qui constitue les prémisses de la justice prédictive (B.).

A. Enjeux de la justice prédictive en termes de traitement de données à caractère personnel

192. Approche de la prédictivité – Les craintes émises s'agissant du développement de traitements algorithmiques de la justice dépendent toutefois de la définition attribuée au terme de « prédictif ». Ainsi les choses diffèrent selon que l'on considère la prédictivité comme un outil d'aide à la décision ou alors comme entrainant la création d'un algorithme liant le juge dans celle-ci.

193. Prédictivité de la justice et données à caractère personnel – Cette question intéresse fortement le sujet des données à caractère personnel dans le procès puisqu'il s'agit de recourir à des logiciels et des algorithmes (legaltech[580]) qui pourront établir des probabilités en se basant sur des bases de données judiciaires. La mise en œuvre de ce dispositif nécessite donc la numérisation de toutes les décisions de justice et leur regroupement au sein de bases de données. Cette consécration de *l'open data* judiciaire appelle certaines garanties. En ce sens, une déclaration commune de la Cour de cassation et du Conseil national des barreaux propose que la collecte et la mise à disposition des données relève de la Cour de cassation et qu'une autorité de régulation soit créé[581].

194. Adoption d'une charte éthique sur l'intelligence artificielle – La Commission européenne pour l'efficacité de la justice a adopté le 4 décembre 2018 une charte éthique relative à l'utilisation de l'intelligence artificielle dans le milieu judiciaire. Elle énonce des principes « cyberéthiques »[582] nécessaires à la bonne maitrise des outils de justice prédictive. La Commission rappelle que les droits fondamentaux devront être protégés et notamment le droit à la protection des données à caractère personnel. Aussi, le système doit garantir l'absence de toute discrimination qui pourrait résulter du traitement des données par

[580] Vient de l'anglais « legal technology » traduit par « Technologies au service du droit ».
[581] T. Coustet, *Open data* judiciaire : le CNB et la Cour de cassation réclament la création d'une instance de régulation, *Dalloz actualité*, 20 mars 2019.
T. Coustet, M. Babonneau, Open data des décisions de justice : le casse-tête judiciaire du 21e siècle, *Dalloz actualité*, 10 janvier 2018.
[582] Commission européenne pour l'efficacité de la justice, Charte éthique européenne d'utilisation de l'intelligence artificielle dans les systèmes judiciaires et leur environnement, AP 4 décembre 2018.
A.A. Hyde, Vers une cyberéthique de la justice « prédictive », *Dalloz IP/IT*, 2019, p. 324.

algorithmes. Comme tout traitement de données, le recours à ces systèmes devra assurer la qualité et la sécurité des données. Ensuite, un principe de neutralité, transparence et intégrité intellectuelle devra permettre au juge de comprendre la solution proposée par le logiciel qui devra toujours l'être dans l'intérêt de la justice. Enfin, la Commission rappelle que le juge doit rester maitre de sa décision, l'algorithme étant là pour éclairer sa décision et non la prescrire. A ce sujet et reprenant les dispositions de la directive police-justice, la loi informatique et liberté dans sa nouvelle rédaction dispose qu'une décision de justice qui implique d'apprécier le comportement d'une personne ne peut reposer sur un traitement automatisé. Aussi, aucune décision ne peut avoir pour seul fondement un traitement de données destiné à « prévoir ou évaluer certains aspects personnels relatifs à la personne »[583].

195. Problématique quant à la protection des données personnelles – La question de la mise en *open data* des décisions de justice soulève nécessairement celle de l'anonymat. Le processus de pseudonymisation laisse une marge d'identificabilité de la personne. Cette marge est-elle envisageable s'agissant de *l'open data* ? La question de l'identification se pose également concernant les professionnels de la justice rendant les décisions ou participant à la justice. Là aussi, le sujet divise et la transposition du règlement européen sur la protection des données a apporté quelques précisions.
Partant de ces constats, la création du fichier « DataJust » marque les prémisses de la mise en œuvre d'une justice dite prédictive.

B. « DataJust », prémisse de la justice prédictive

196. Fichier de traitement par algorithme des données – La création de « DataJust » pose une nouvelle pierre dans la nomenclature des fichiers judiciaires[584]. Ainsi, aux côtés des fichiers de renseignement, des fichiers de constatation ou d'identification on peut désormais citer les fichiers de traitement par algorithme des données. Il convient d'observer en détails le texte du décret portant création du fichier (1°) pour s'interroger sur les questions soulevées par la concrétisation de l'usage des algorithmes en matière judiciaire (2°).

1° Le décret portant création de « DataJust »

[583] Art. 95 de la loi informatique et libertés.
[584] Rappelons que le choix a été fait d'utiliser le terme de « fichier judiciaires » de manière générique et que ce dernier renvoie à tous les traitements mis en œuvre par les autorités judiciaires ou auxquels ont recours les autorités judiciaires dans l'exercice de leurs fonctions. Les fichiers prennent ici une nouvelle dimension.

197. Finalités du fichier – Créé par décret du 27 mars 2020[585], placé sous l'autorité du ministère de la Justice et autorisé pour une durée initiale de deux ans, le traitement de données « DataJust » a pour finalité de développer un algorithme des données issues de décisions rendues par les formations civiles des juridictions judiciaires et par les juridictions administratives. Le décret exclut donc les décisions sur intérêts civils rendu dans une procédure pénale. Plus précisément, ce fichier a d'abord pour vocation d'informer les parties quant à l'éventuelle indemnisation à laquelle elles peuvent prétendre, avec un but annoncé de favoriser le règlement amiable des litiges. En outre, il doit constituer une base informative à destination des juges qui, en plus de la jurisprudence, pourront alors observer la position de leurs pairs sur des conflits similaires en termes d'indemnisation. Enfin, ce traitement a pour finalité de créer un référentiel en matière d'indemnités versées en réparation des préjudices corporels. L'algorithme peut alors proposer une indemnité en fonction d'une situation donnée et des précédents sur des affaires similaires. C'est ce dernier point qui soulève de vives interrogations.

198. Données concernées – Aux côtés des traditionnelles données relatives à l'identité de la personne, le fichier doit contenir des données relatives au préjudice telles que la description des différentes atteintes et dommages, les dépenses attachées à ces préjudices, des données relatives à la vie professionnelle de l'individu et les éventuelles atteintes à celle-ci, ainsi que les éventuels avis et expertises réalisés. Ces données sont conservées le temps nécessaire à la création de l'algorithme dans la limite de deux ans. Ont accès, dans l'immédiat, à ces données les agents dépendant du ministère de la justice. Le traitement « DataJust » doit être alimenté par des données de procédures d'appel relatives aux décisions rendues entre 2017 et 2019 à partir des bases de données « Ariane »[586] et « JuriCA »[587], puis au fur et à mesure avec de nouvelles décisions.

L'article 6 du décret précise qu'au vu « des efforts disproportionnés » que cela engendrerait, le droit d'information ne s'applique pas à ce fichier[588]. Les individus peuvent faire jouer leur droit d'accès indirect.

---

[585] Décret n° 2020-356 du 27 mars 2020, portant création d'un traitement automatisé de données à caractère personnel dénommé « DataJust ». Voir, Y. Meneceur, DataJust face aux défis de l'intelligence artificielle, *JCP G*, 28 septembre 2020, n° 40, doctr. 1087.

[586] « Arianne » est une base de données comprenant les décisions du conseil d'Etat, du tribunal des conflits et certains arrêts des Cours administratives d'appel.

[587] « JuriCA » est une base de données comprenant l'ensemble des arrêts rendus par les Cour d'appel et les décisions juridictionnelles prises par les premiers présidents de cours.

[588] Telle que prévu par l'article 14-5 b) du règlement général sur la protection des données.

Ainsi, d'un décret assez bref sont nées les prémisses d'une justice prédictive soulevant de nombreuses interrogations.

199. Limites quant à la portée – Il faut mentionner que dans l'immédiat, l'usage de « DataJust » est limité à la fixation des indemnités en matière de préjudices corporels. Il s'agirait donc d'un référentiel basé sur les cas concrets et les décisions rendues en la matière. Cela n'est pas sans rappeler la nomenclature Dintilhac créé en 2005 et qui détaille de manière exhaustive les différents postes d'indemnisation en matière de préjudices. Toutefois, à la différence de la nomenclature Dintilhac qui répertorie les postes de préjudice, « Datajust » propose par le biais de calculs algorithmiques, des indemnités. Ce recours aux algorithmes et à l'intelligence artificielle n'est pas sans soulever certaines interrogations.

2° Interrogations soulevées quant à la concrétisation de l'usage des algorithmes en matière judiciaire

200. Craintes face au développement de la justice prédictive – De manière générale, les arguments défavorables le plus souvent formulés à l'encontre du développement d'une justice dite « prédictive » reposent sur les craintes de voir le juge lié par la jurisprudence antérieure ne disposant alors plus de son réel arbitre et entrainant, de ce fait, une justice figée. Parmi les arguments positifs, il ressort la volonté d'harmoniser le système judiciaire et de favoriser les modes de règlement alternatifs puisque l'issue du procès pourrait être anticipée. Ce système pourrait au demeurant redonner du poids aux décisions prises par les juges du fond puisqu'ils statueraient en fonction de l'interprétation de la Cour de cassation mais aussi en fonction des décisions prises, avant eux, par leurs pairs[589].

201. Avis de la CNIL sur le projet « DataJust » – La Commission nationale de l'informatique et des libertés a rendu un avis favorable s'agissant du projet de décret portant création de « DataJust »[590]. Toutefois, en raison de la nature sensible des données concernées, elle appelle à une grande vigilance s'agissant des éventuelles évolutions dans la finalité du traitement. Aussi, au vu du projet annoncé d'un accès qui serait à terme ouvert au public, la

[589] E. Buat-Ménard, La justice dite « prédictive » : pré requis, risques et attentes - l'expérience française, *op. cit.*, p. 269. L'auteur fait référence à la « jurisprudence horizontale ».
[590] Délibération CNIL n° 2020-002 du 9 janvier 2020 portant avis sur un projet de décret en Conseil d'Etat portant création d'un traitement automatisé de données à caractère personnel dénommé « DataJust » (demande d'avis n° 19020148).

Commission s'interroge sur l'opportunité d'adopter une loi spécifique encadrant le traitement. S'agissant des données collectée ou plus exactement, transmises par la Cour de cassation et le Conseil d'Etat, la CNIL rappelle que les données relatives à l'identité des individus seront partiellement pseudonymisées avant la transmission. S'agissant de la dérogation prévue au droit d'information relatif au traitement, la CNIL suggérait toutefois que le décret précise qu'une information générale serait délivrée sur le sujet[591]. Pour conclure, la CNIL semble donner son aval sur la création du dispositif appelant néanmoins à la prudence du fait de la nature des données traitées ce qui s'inscrit dans les recommandations habituelles de la cette dernière. Comme pour tout traitement, la Commission s'interroge sur les évolutions du fichier en termes de finalités qui pourraient ne plus correspondre à la finalité initiale.

202. Sur les apports du fichier – Le traitement « DataJust » peut apporter des avancées positives si l'on considère l'algorithme comme une aide à la décision du juge et non comme un outil d'intelligence artificielle le remplaçant. Ainsi, l'idée de faciliter pour le juge décideur, l'accès aux données jurisprudentielles et aux précédents similaires au litige qu'il doit trancher, peut apparaitre comme bénéfique de prime abord. Sur les traces de la nomenclature Dintilhac, « DataJust » constitue alors une évolution de celle-ci en ce qu'il permet d'harmoniser l'indemnisation des préjudices corporels en donnant au juge, au vu de son affaire, le montant attribué pour des affaires similaires. Ainsi, la prise de décision et avant cela l'éventuel règlement amiable des litiges pourraient être facilités.
Cette approche ne permet donc pas de conclure en l'avènement d'une justice artificielle et déshumanisée mais s'interprète comme une évolution de la manière de juger, rendue plus facile grâce aux évolutions technologiques que permet notre époque.

203. Craintes légitimes quant au recours aux algorithmes – La création de « DataJust » soulève quoi qu'il en soit des craintes légitimes. Tout d'abord, c'est évidement la question de la sécurité des données traitées qui se pose. Bien qu'il soit prévu une pseudonymisation des données d'identification, on peut s'interroger sur la réelle protection des individus concernés en raison des failles de ce dispositif[592] et ce notamment dans la perspective d'étendre l'accès au fichier aux parties.

[591] Sur l'avis de la CNIL, voir, C. Crichton, Création de « DataJust », un algorithme prédictif d'évaluation du préjudice, *Dalloz IP/IT*, 2020, 209.
[592] V. *infra* n°427.

Aussi, c'est l'évolution plus générale du recours à l'interprétation algorithmique des données de procédure qui peut soulever certaines craintes légitimes. On peut imaginer que l'adoption du décret relatif à « DataJust » s'agissant de l'évaluation des préjudices corporels, ne soit qu'une première étape dans cette évolution et cette intégration de l'intelligence artificielle dans le procès.

En cela, certain gardes fous existent interdisant notamment que des décisions relatives à l'analyse de la personnalité ou produisant des effets juridiques à l'égard des individus reposent seulement sur un traitement automatisés[593]. Néanmoins, on peut s'interroger sur l'impact de l'analyse algorithmique sur la décision du juge quand bien même celle-ci ne reposerait pas exclusivement sur elle. En tant qu'outil d'aide à la décision, le recours à l'intelligence artificielle pourrait-il être envisagé pour d'autres contentieux ? Bien que le juge ne statuerait pas sur ces seuls algorithmes, quelle serait, par exemple, en pratique leur place dans l'acquisition par celui-ci de son intime conviction ?

Si le recours à « DataJust » va nécessairement opérer une harmonisation dans l'indemnisation des préjudices, on peut s'interroger sur les risques liés à la consécration d'une « barémisation »[594] en la matière. A ce sujet les avis diffèrent. Au demeurant, l'accès au fichier par les particuliers pourrait avoir un effet dissuasif sur la saisine du juge.

On peut donc regrouper les fichiers judiciaires en différentes catégories bien qu'il apparaisse évident que certains disposent de finalités multiples. Après avoir étudié les motivations qui ont poussé au développement du nombre de fichiers judiciaires, il convient de s'interroger sur les normes qui encadrent ces derniers.

Section 2 : Le cadre règlementaire relatif aux fichiers judiciaires

204. Absence de régime propre aux fichiers judiciaires – Les fichiers judiciaires soulèvent de manière récurrente des interrogations notamment concernant le contrôle opéré sur leur création. Il n'existe pas de régime juridique propre aux fichiers judiciaires, et un tel régime ne semble pas envisageable au vu de la diversité des fichiers et de leur finalité[595]. Toutefois, l'étude de ces derniers permet de mettre en exergue certains principes qui tendent à s'appliquer à leur création et à leur gestion. Par ailleurs, le développement du droit à la protection des

[593] Ar. 95 de la loi informatique et libertés.
[594] S. Merabet, « DataJust » et l'effet papillon, *Revue pratique de la prospective et de l'innovation*, octobre 2020, n°2.
[595] Voir, D. Larbre, « Les fichiers de police : une catégorie juridique incertaine ? », *Terminal, technologie de l'information*, culture et société, *op. cit.*

données personnelles a nécessairement des répercussions s'agissant des fichiers judiciaires. Il s'agit ici de s'intéresser à la question des normes qui encadrent la création des fichiers. Les interrogations liées à la gestion et à l'utilisation seront abordées dans la seconde partie. En ce qui concerne la question de la création des fichiers judicaires, cette dernière est soumise en particulier à la loi informatique et libertés du 6 janvier 1978 (§1.), à un contrôle de légalité opéré par le conseil d'Etat (§2.), à un contrôle de constitutionnalité (§3.), ainsi qu'au contrôle des juges supranationaux (§4.).

§1. La loi informatique et libertés

205. Loi informatique et libertés – La création même de fichiers judiciaires doit répondre à certaines obligations fixées notamment par la loi informatique et libertés. Cette loi a été à plusieurs reprises modifiée notamment en 2018 lors de sa mise en conformité avec le droit européen. Entrée en vigueur le 1er juin 2019 suite à l'adoption du décret du 29 mai 2019[596], la loi informatique et libertés dans sa nouvelle version est venue modifier de manière substantielle le rôle et les attributions de la CNIL. C'est notamment le cas en matière de création et contrôle de fichiers. Elle comprend des dispositions communes et traite ensuite distinctement les traitements en fonction de leur nature et de la norme de laquelle ils relèvent. Dans sa nouvelle rédaction, le législateur met fin au régime de déclaration antérieur posé à l'ancien article 22 de la LIL et modifie le régime d'autorisation. Avec la transposition du droit européen, le traitement des données à caractère personnel doit désormais répondre à deux niveaux de réglementation. Il faut comprendre toutefois que si la transposition du règlement européen sur la protection des données a, sur certains points, remplacé les dispositions internes, s'agissant d'autres points le droit national trouve toujours à s'appliquer en complément du droit supra national. C'est notamment le cas s'agissant des données relatives aux infractions. Pour une meilleure analyse du sujet, il convient néanmoins de s'intéresser au régime antérieur à la transposition, puisque les fichiers existants l'ont été sous ce régime. Rappelons que la loi informatique et libertés est le premier texte législatif qui sous couvert de protection des données personnelles des individus est venu imposer des obligations et des responsabilités en matière de traitement de données. Pour rappel, cette dernière a fait suite au scandale lié au projet « Safari » en 1970. Face aux craintes pesant sur la sécurité des données personnelles des individus, le législateur pose en 1978 un cadre légal en matière de traitement

[596] Décret n° 2019-536 du 30 mai 2019 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

de données à caractère personnel et crée une autorité administrative indépendante chargée de veiller au respect des dispositions fixées. Il s'agit de la Commission nationale de l'informatique et des libertés (CNIL). Cette dernière est composée d'un collège formé par 18 commissaires issus d'entités distinctes. Au niveau interne, la CNIL occupe un rôle important en termes de création de fichiers en fixant notamment les modalités de création en fonction de la catégorie de données concernées. Son rôle a toutefois été revu à la baisse lors de la réécriture de la loi informatique et libertés notamment en ce qui concerne son pouvoir initial d'autorisation des traitements. La CNIL conserve un rôle en matière de création de fichiers (A.) malgré le maintien résiduel du régime d'autorisation (B.).

A. Le rôle de la CNIL en matière de création de fichiers

206. Création de la CNIL – La CNIL a depuis sa création en 1978 un rôle d'information, de contrôle et de sanction. Plus précisément, sa mission première est de renseigner les personnes sur leurs droits et obligations quant au traitement de données personnelles. A ce titre, elle a souvent été appelée à se prononcer avant l'adoption d'un projet de loi relatif à la protection des données à caractère personnel afin de rendre un avis. Elle intervient également d'elle même en rendant très régulièrement des délibérations au sujet de traitements de données. Aussi, la CNIL assure le droit d'accès aux données des individus auxquels elle se substitue dans les démarches. Ensuite, la CNIL a pour mission de recenser les fichiers et de faire appliquer la réglementation définie par la loi informatique et libertés en matière de création de traitement de données personnelles. Avant la transposition des normes européennes, la CNIL avait des prérogatives avant toute mise en œuvre de traitement nouveau. Ainsi, toute création de fichier devait en fonction de la nature des données concernées répondre à une obligation de déclaration ou dans certains cas d'autorisation. Cette autorisation concernait notamment les données dites « sensibles » au sens de la loi. Ensuite, la CNIL assure une mission de contrôle des systèmes de traitement de données. Sur commission de son président elle opère un contrôle d'applications bureautiques. Elle instruit également les plaintes déposées à l'encontre de certains organismes. De manière générale, la CNIL surveille les systèmes de traitement et veille à ce que ces derniers respectent dans la durée les dispositions de la LIL. Enfin, la formation contentieuse de la commission peut prononcer des sanctions à l'encontre des responsables de traitements qui contreviendraient aux dispositions de la LIL. Ces mesures peuvent être prononcées en urgence. Le président de la commission dispose du pouvoir de

dénoncer les violations au procureur de la République. Ce pouvoir de contrôle et de sanction a quant à lui été renforcé lors de la transposition des normes européennes. Finalement, la CNIL a connu un allégement des prérogatives a priori par la suppression des formalités préalables à la mise en œuvre de traitements (1°). La Commission conserve ses prérogatives relatives au régime d'avis (2°).

1° Un allégement des prérogatives a priori par la suppression des formalités préalables à la mise en œuvre de traitements

207. Suppression du régime d'autorisation préalable – De manière générale, la transposition du règlement général sur la protection des données a mis fin a certaines prérogatives de la CNIL en matière de création de fichiers et notamment à son pouvoir d'autorisation. La loi informatique et libertés dans sa nouvelle rédaction a également abrogé les dispositions relatives aux formalités préalables telles que le régime de déclaration auprès de la CNIL. Indiscutablement, la CNIL a vu ses attributions, a priori, limitées. La réforme de la loi informatique et liberté a abrogé les anciens articles 23 et 24 de la loi relatifs au régime de déclaration auprès de la CNIL de tout traitement qui ne serait pas susceptible de porter atteinte à la vie privée. Aussi, est abrogé l'article 25 relatif au régime d'autorisation par la CNIL des traitements de données dites sensibles telles que visées par l'article 6 de la loi et notamment les traitements relatifs aux infractions, condamnations et mesures de sureté. Etaient également visés les traitements de données biométriques. Désormais, la nouvelle rédaction de la loi consacre son titre III aux dispositions relatives aux traitements relevant la directive du 27 avril 2016 dite « police-justice » qui tend à définir les régimes applicables en matière de données pénales. Pour rappel, la directive avait été transposée en droit interne avant le règlement européen et avait été codifiée aux articles 70-1 et suivants de la loi informatique et libertés. Suite à la transposition du règlement européen sur la protection des données la loi a été de nouveau modifiée et les dispositions relatives à la directive police-justice ont été recodifiées aux articles 87 et suivants du titre III de la nouvelle loi. L'ordonnance du 12 décembre 2018 portant transposition des dispositions du RGPD a repris à l'identique les dispositions de la directive police-justice et n'a inséré qu'un nouvel article.

2° Le régime d'avis

208. Accentuation du régime d'avis – La CNIL est amenée à émettre des avis lors de délibérations de son propre chef ou dans le cadre de certains traitements. Les articles 31 et 32 de la loi informatique et libertés prévoient une procédure de demande d'avis préalable dans le cadre de certains types de traitements mis en œuvre pour le compte de l'Etat ou par des organismes privés gérant un service public. Cette demande d'avis doit nécessairement précéder toute mise en œuvre de traitement relatif à la sûreté de l'Etat, la défense ou la sécurité publique, à la prévention, la recherche, la constatation ou la poursuite d'infractions pénales, ou à l'exécution de condamnations ou de mesures de sûreté. Elle est également requise en matière de traitement portant sur des données biométriques. L'avis de la CNIL devait aussi être demandé avant tout traitement visant le recensement de la population ou les télé-services de l'administration. Il ne s'agit toutefois là que d'un simple avis. Ce dernier doit néanmoins accompagner tout projet de décret ou d'arrêté portant autorisation de création dudit traitement. La CNIL a été amenée à rendre de nombreux avis relatifs à la création de fichiers de police dans lesquels elle « valide » les dispositifs et parfois rend des avis plus nuancés voir alarmants.

209. La validation du projet de décret portant création du FAED – Lors de la création du FAED par décret du 8 avril 1987, le projet de création du fichier a fait l'objet d'une délibération de la CNIL le 14 octobre 1986[597]. La commission a retenu que le cadre fixé et les garanties apportées étaient suffisants et « de nature à garantir les libertés individuelles ou publiques et le respect de la vie privée ». Cette dernière a donc rendu un avis positif concernant le projet de création.

210. La validation du fichier informatisé des personnes des services de renseignement – Bien plus tôt, la commission s'était prononcée sur un projet de mise en œuvre d'un fichier informatisé par la direction centrale des renseignements généraux. Dans sa délibération en date du 30 novembre 1982[598], la CNIL avait là aussi validé le dispositif en émettant néanmoins quelques réserves. La commission a considéré que le recueil de données dans ce fichier était nécessaire à l'accomplissement par les services de renseignement de leur

[597] Délibération CNIL n°86-102 du 14 octobre 1986 concernant un projet de décret relatif au fichier automatisé des empreintes digitales géré par le Ministère de l'Intérieur.
[598] Délibération CNIL n°82-199 du 30 novembre 1982 portant avis sur la mise en œuvre du fichier informatisé des personnes par la direction centrale des renseignements généraux du Ministère de l'Intérieur et de la Décentralisation. La CNIL s'est rarement prononcée sur les fichiers relatifs aux services de renseignements avant le décret du 14 octobre 1991 les rendant « officiels ».

mission[599]. Toutefois, la commission précise que de par la nature des données recueillies, ces dernières doivent être accessibles à un nombre restreint de personnes et ne doivent avoir pour seul but que l'information du gouvernement chargé du maintien de l'ordre public et de la sûreté de l'Etat. Aussi, le droit au respect de la vie privée impose de ne pas transmettre les données à des personnes privées. De plus, la commission mentionne que les données ne doivent être conservées que le temps nécessaire à leur utilité. Enfin, elle précise que dans le cadre d'enquêtes administratives qui seraient menées par les services de renseignements, ces dernières ne doivent pas s'appuyer sur des données relatives aux origines ethniques, aux opinions politiques ou religieuses ou à l'appartenance syndicale des personnes concernées[600]. Le projet dont il question avait pour vocation de développer un outil relatif au fichage en matière de lutte contre le terrorisme. Cette extension[601] avait nécessairement pour conséquences d'augmenter le nombre de personnes fichées par les services de renseignement et les données collectées. La commission a donc appelé à une très grande prudence concernant l'accès à cette application.

211. Un avis nuancé relatif au FIJAIS – Dans sa délibération du 8 novembre 2007[602] relative au projet d'extension du nombre de personnes pouvant avoir accès au FIJAIS, la Commission a rendu un avis nuancé. Ce projet visait à ouvrir l'accès au fichier aux autorités administratives alors qu'il était jusqu'à présent accessibles par les seules autorités judiciaires. La commission avait émis quelques réticences concernant le projet de décret[603]. Elle soulevait par exemple l'absence de précisions du décret concernant les éventuelles conséquences de la consultation par l'Administration des données du FIJAIS. Dans son rapport, la CNIL rappelle l'article 10 de la loi informatique et libertés de 1978 aux termes duquel « aucune décision produisant des effets juridiques à l'égard d'une personne ne peut être prise sur le seul fondement d'un traitement automatisé de données destiné à définir le profil de l'intéressé ou à évaluer certains aspects de sa personnalité ». Toutefois, malgré de telles réticences, le décret fut adopté le 6 octobre 2008.

---

[599] Ces missions sont fixées par l'article 7 du décret n°67-198 du 14 mars 1967 soumis au secret défense.
[600] Ces dispositions sont applicables sous réserve de procédures particulières d'habilitation au secret défense.
[601] Cette application désignée « violence-Attentats-Terrorisme » est alimentée par les services du renseignement ainsi que par ceux de la direction centrale de la police judiciaire, la direction de la surveillance du territoire ainsi que par la direction générale de la sécurité extérieure. La CNIL a donc considéré que de par le nombre de personnes concernées, l'augmentation du nombre de données collectées et la finalité de cette application, elle constituait un nouveau traitement.
[602] Délibération CNIL n°2007-326 du 8 novembre 2007 relative au projet de décret n°2008-1023 du 6 octobre 2008 relatif au FIJAIS.
[603] Voir à ce sujet l'article de G. J. Guglielmi, « Comment s'asseoir sur une recommandation de la CNIL. « *Le FIJAIS bouge, il est bien vivant...* », sur site, www.guglielmi.fr., 9 octobre 2008.

212. Un avis en demi-teinte relatif au FIJAIT – Créé sur un format proche du FIJAIS, son pendant en matière de terrorisme a fait l'objet d'un avis tout aussi nuancé de la CNIL. Dans sa délibération en date du 25 avril 2015[604], la commission émettait un avis réservé sur le fait que certains représentants de l'Etat puissent avoir accès aux données du FIJAIT dans le cadre de recrutements. Comme pour le FIJAIS, elle recommandait un accès strictement limité à certaines personnes dans le cadre de missions bien définies.

213. Un appel à la prudence rendu concernant le FPR – La diversité du fichier des personnes recherchées a également amené la commission nationale de l'informatique et des libertés à se prononcer. Dans son avis du 12 novembre 2009[605] qui a précédé l'adoption du décret du 28 mai 2010, cette dernière a alerté sur les risques d'une telle « obsolescence »[606]. Une telle diversité doit selon elle s'accompagner de garanties strictes notamment concernant l'accès au fichier et donc la procédure d'habilitation des personnes concernées. Elle conseille même que soit mise en place une méthode de « traçabilité ». Le gouvernement avait d'ailleurs pris acte de cette remarque et modifié le décret afin que soit prévu un enregistrement des consultations du fichier.

214. Un avis alarmant concernant le TAJ – Le traitement des antécédents judiciaires (TAJ) fusion en 2011 du système de traitement des infractions constatées (STIC) et du système judiciaire de documentation et d'exploitation (JUDEX) a également fait l'objet de vives critiques de la part de la CNIL. Dans un premier rapport remis au premier ministre le 20 janvier 2009[607], la commission avait déjà dénoncé plusieurs « défaillances » relatives au fonctionnement du STIC. Les critiques portaient sur les erreurs de saisie dans les dossiers liées à des facteurs humains mais aussi matériels tenant à des logiciels inadaptés. Deuxièmement, la CNIL dénonçait l'absence de mise à jour systématique des données notamment en cas de classement sans suite, relaxe, non-lieu ou acquittement. Ensuite, le rapport fait état de la méconnaissance par certains parquets des dispositions de la loi LOPPSI

[604] Délibération CNIL n°2015-119 du 7 avril 2015 portant avis sur un projet de dispositions législatives visant à créer un fichier national des auteurs d'infractions terroristes (FIJAIT), rendu public sur demande du Gouvernement.
[605] Délibération CNIL n°209-587 du 12 novembre 2009.
[606] Le terme « d'obsolescence » a été utilisé dans un rapport rédigé par les députés D. Batho et J.A. Benisti relatif aux fichiers de police. Dans ce rapport, les auteurs dénoncent « l'obsolescence technique » du fichier. Rapport d'information n°4113 enregistré le 21 décembre 2011.
[607] Rapport CNIL du 20 janvier 2009, conclusions du contrôle du système de traitement des infractions constatées.
Voir à ce sujet, M. Lena, Les atteintes liées à l'entrée en vigueur du traitement des antécédents judiciaires, *AJ pénal*, 2013, p. 635.

II imposant la nomination d'un magistrat référent en matière de mise à jour des fichiers. Enfin, la commission critiquait le fait que les enquêtes administratives permettant par exemple l'accès à certaines professions soient réalisées sur des données parfois erronées[608]. Censée apporter de nouvelles garanties, la création du TAJ a néanmoins soulevé de vives inquiétudes notamment liées à la reprise des informations contenues dans les fichiers STIC et JUDEX qu'il remplace. Dans un rapport rendu le 13 juin 2013[609], la CNIL avait dénoncé la reprise de données erronées sans que ne soient effectuées des mises à jour sur les deux fichiers. Cette reprise de données doit faire l'objet d'une vérification notamment concernant les données les plus sensibles. La CNIL a aussi émis des critiques concernant les nouvelles dispositions de l'article R. 40-26 du CPP au terme desquelles le TAJ peut collecter des données photographiques « comportant des caractéristiques techniques permettant le recours à un dispositif de reconnaissance faciale ». Ce mécanisme de reconnaissance faciale pourra être effectué à partir d'images recueillies par les caméras de vidéosurveillance ce qui, pour la CNIL, soulève des interrogations en termes d'atteintes à la vie privée[610].

B. Le maintien résiduel d'un régime d'autorisation

215. Conservation, par exception, du régime d'autorisation – S'agissant de certaines catégories de données à caractère personnel, la réforme a conservé des formalités préalables à la mise en œuvre de tout traitement. C'est le cas notamment des données dites sensibles pour lesquelles tout traitement doit être autorisé par le Conseil d' Etat (1°) ou du traitement des données pénales qui reprend et accentue les dispositions de la directive police/justice (2°). Face à cette diminution de pouvoirs a priori de la CNIL, le législateur a néanmoins renforcé les obligations incombant au responsable du traitement (3°).

1° Le traitement de données sensibles soumis à autorisation du Conseil d'Etat

216. Autorisation de traitement s'agissant des données sensibles – Le règlement européen laisse une marge de manœuvre aux Etats dans la transposition des dispositions qu'il édicte. Ainsi, le législateur français a choisi de maintenir les formalités préalables pour certaines

[608] A ce sujet, le rapport fait le constat que les procureurs de la République chargés de ces contrôles au vu de l'article 230-8 du CPP ne disposent bien souvent pas des accès aux fichiers.
[609] Rapport CNIL du 13 juin 2013 adopté en assemblée plénière relatif au contrôle des fichiers d'antécédents du ministère de l'intérieur.
[610] Voir à ce sujet, M. Lena, Les atteintes liées à l'entrée en vigueur du traitement des antécédents judiciaires, *op . cit.*, p. 635.

données. C'est le cas notamment des traitements portant sur le numéro NIR[611], les traitements de données génétiques ou biométriques ou les traitements intéressant la sureté de l'Etat ou qui ont pour objet la prévention ou la répression des infractions pénales.

217. La mise en œuvre de traitements comportant des données génétiques ou biométriques – S'agissant des traitements intéressant les procédures judiciaires comme le traitement des données génétiques ou biométriques, le nouvel article 32 de la LIL soumet la mise en œuvre à autorisation du Conseil d'Etat pris après avis motivé et publié de la CNIL, étant précisé que ces traitements sont nécessairement mis en œuvre pour le compte de l'Etat dans un but d'authentification ou de contrôle d'identité des personnes. L'ancien article 25 de la LIL soumettait ce traitement à autorisation de la CNIL. Il faut également rappeler que la LIL dans sa nouvelle rédaction ajoute à la liste des données dites sensibles les données génétiques, biométriques[612].

218. La mise en œuvre de traitements relatifs aux infractions et condamnations – Concernant les données liées aux infractions et condamnations, les nouvelles dispositions issues du règlement européen apportent des précisions tant sur le régime que sur le terme même. Mettant fin à la jurisprudence du Conseil d'Etat, l'article 46 de la LIL vient préciser que les dispositions s'appliquent aux seules condamnations pénales là où le Conseil d'Etat avait estimé qu'elles visaient également les condamnations civiles[613]. La nouvelle loi encadre donc plus strictement le traitement des données d'infractions et de condamnations mais assouplit le régime qui y est attaché[614]. En effet, l'article liste les personnes susceptibles de recourir au traitement des données visées et ajoute les personnes morales de droit privé collaborant au service public de la justice et les réutilisateurs des données publiques issues des décisions tant qu'elles ne permettent pas de réidentifier les personnes concernées[615].

[611] Art. 30 de la loi informatique et libertés.
[612] Art. 6 nouveau de la loi informatique et libertés.
[613] CE, 28 juillet 2004, n°262851.
[614] Voir en ce sens, M. Bourgeois, M. Moine, La nouvelle loi informatique et libertés : des changements substantiels après le RGPD, *JCP E*, 5 juillet 2018, n°27.
[615] Ces personnes sont donc ajoutées à celles déjà visées dans l'ancien régime à savoir les autorités publiques, les juridictions…visées à l'ancien article 9 de la loi informatique et libertés. Le terme de personnes morales de droit privé collaborant au service public de la justice vise notamment les associations de victimes.

2° La reprise et l'accentuation des dispositions de la directive police-justice en matière de traitement des données pénales

219. Traitement de données pénales –Le traitement des données pénales relève désormais des dispositions issues de la directive police-justice de 2016 qui abroge la directive du 27 novembre 2008 relative à la coopération policière et judiciaire. L'objectif annoncé était d'harmoniser le régime en matière de traitement des données pénales entre les différents membres et garantir une meilleure protection notamment lors des échanges de données. Ainsi l'article 87 de la loi informatique et libertés dans sa nouvelle version précise que les dispositions s'appliquent aux traitements de données à caractère personnel relatifs à la prévention, la détection des infractions, leur poursuite et l'exécution des condamnations[616]. Tout traitement mis en œuvre pour le compte de l'Etat doit être prévu par une loi ou un règlement et autorisé par arrêté après avis de la CNIL[617]. Finalement, sur ce point, la directive a réaffirmé le principe préexistant d'autorisation préalable. Elle va toutefois plus loin en prévoyant que dans le cas où le traitement est susceptible de porter atteinte aux droits ou libertés individuelles, ce dernier doit faire l'objet d'une analyse d'impact préalable. Elle est dans le cas des fichiers de police jointe à la demande d'avis adressée à la CNIL. La directive réaffirme aussi un principe existant en précisant que les données collectées par les autorités judiciaires dans le cadre de poursuites, d'enquêtes et de condamnations ne peuvent être utilisées que pour la finalité pour laquelle elles ont été collectées. Toute utilisation pour un autre motif doit avoir été prévue par la loi interne ou le droit de l'Union européenne[618] et doit être nécessaire et proportionné[619]. Il s'agit ici du principe de finalité déjà présent de l'ancien régime. Là où la directive va plus loin que le dispositif antérieur c'est en matière de données dites sensibles. Le traitement de données sensibles tel que visé à l'article 6 ne peut être possible que s'il est nécessaire, l'article 87 de la loi faisant référence à une « nécessité absolue ». La directive pose également une interdiction « absolue ». En effet, est prohibé le fait de prendre une décision de justice « impliquant une appréciation sur le comportement d'une personne » qui trouverait son fondement sur un traitement automatisé. Il a toutefois été reproché dès le projet de loi de transposition une absence de clarification des dispositions de la directive police-justice. Reprenant les dispositions de la directive telles quelles, certains ont considéré que l'ancien article 70-1 (et donc le nouvel article 87) de la loi informatique et

[616] Art. 87 de la loi informatique et libertés.
[617] Art. 31 de la loi informatique et libertés.
[618] Art. 91 de la loi informatique et libertés.
[619] Art. 92 de la loi informatique et libertés.

libertés n'apportait pas de réelles précisions quant à son champ d'application, ce dernier visant une certaine finalité (« prévention et détection des infractions… ») et les personnes mettant en œuvre le traitement (« les autorités compétentes »)[620].

3° Le renforcement des obligations incombant au responsable du traitement

220. Obligations incombant au responsable – Le traitement des données pénales relève désormais des dispositions issues de la directive police-justice, la loi informatique et libertés dans sa nouvelle rédaction crée des obligations pour le responsable du traitement de tenue de registre et journal d'opérations. L'article 100 de la loi prévoit en effet que le responsable d'un traitement ou le sous-traitant doivent tenir un registre des activités notamment s'agissant des données sensibles. Le document doit mentionner la base légale du traitement ainsi que les éventuels transferts de données et le cas échéant si ce dernier recours aux méthodes de profilage. Le but est d'apporter de meilleures garanties de protection de ces données. Dans la même optique, l'article 101 prévoit la tenue pour chaque traitement automatisé, d'un journal des opérations. Celui-ci mentionne toute collecte, modification, consultation, communication, interconnexion et effacement des données. Ces nouvelles dispositions vont beaucoup plus loin que le dispositif antérieur en créant un réel suivi des données permettant de tracer ces dernières et d'identifier les différents acteurs qui prennent connaissance de celles-ci. La loi précise que ce document mis à la disposition de la CNIL permet un contrôle de la licéité du traitement ainsi qu'un autocontrôle et une meilleure sécurité des données. On perçoit ici l'accentuation du rôle de la CNIL en termes de contrôle a posteriori des fichiers.
Les décrets portant création de fichiers de police peuvent aussi être soumis au contrôle de légalité du Conseil d'Etat.

§2. Le contrôle de légalité opéré par le Conseil d'Etat

221. Contrôle de légalité – La création des fichiers de police est soumise « au regard des juges »[621] et leur fonctionnement à leur « surveillance »[622]. Le Conseil constitutionnel dans une jurisprudence constante rappelle « qu'il appartient au législateur, dans le cadre de sa

[620] Voir par exemple, O. Tambou, Que retenir du projet de loi relatif à la protection des données personnelles ? Partie II : l'amélioration relative du régime des traitements pénaux par la transposition de la directive n°2016/680, *RLDI* 2018/146, 1er mars 2018,
[621] G. Begranger, Le contrôle des fichiers de police par les juges, *AJ Pénal*, 2014, p. 176.
[622] *Ibid.*

compétence, d'assurer la conciliation entre, d'une part, la sauvegarde de l'ordre public et la recherche des auteurs d'infractions, toutes deux nécessaires à la protection de principes et de droits de valeur constitutionnelle et, d'autre part, le respect des autres droits et libertés constitutionnellement protégés »[623]. Les juges suprêmes opèrent donc un contrôle de légalité sur les textes portant création de fichiers de police. Le Conseil constitutionnel a, dans un considérant de principe très largement admis, jugé que pour ne pas méconnaitre le droit au respect de la vie privée « la collecte, l'enregistrement, la conservation, la consultation et la communication de données à caractère personnel doivent être justifiés par un motif d'intérêt général et mis en œuvre de manière adéquate et proportionnée à cet objectif »[624]. Le Conseil d'Etat opère un contrôle de légalité des fichiers de police créés par voie réglementaire. Dans une décision d'assemblée du 26 octobre 2011[625], il a jugé que le traitement de données à caractère personnel dans les fichiers constitue une ingérence dans le droit au respect de la vie privée. A ce titre, ces traitements doivent être adéquats et proportionnés en fonction de leur finalité.

222. L'exemple du contrôle de légalité du fichier CRISTINA – Dans une décision du 16 avril 2010[626], le Conseil d'Etat a eu à se prononcer sur la légalité du fichier CRISTINA dans le cadre d'une requête en annulation du décret portant création du fichier ainsi que du décret portant dispense de publication de celui-ci. En effet, étant classé secret défense, le décret portant création du fichier n'a pas été publié. Sur la question de la légalité du fichier, le Conseil d'Etat a rejeté les demandes d'annulation du décret portant création du fichier et du décret portant dispense de publication de celui-ci. Sur la légalité externe, le Conseil d'Etat rappelle qu'il est possible de prononcer la dispense de publication d'un décret notamment quand celui-ci intéresse la sûreté de l'Etat ou la défense et que les données contenues dans le fichier concerné sont en adéquation avec sa finalité. Aussi, une décision de dispense n'a pas à être motivée. S'agissant du décret créant le fichier, le Conseil d'Etat retient que le projet qu'il a adopté est en adéquation avec le décret final. Sur la légalité interne, le Conseil d'Etat retient que la dispense de publication du décret est justifiée par la nature des données et la finalité du fichier qui intéresse la défense et rejette l'argument de violation du droit au recours effectif. Aussi, les requérants invoquaient une violation du principe de sécurité juridique et du droit au respect de la vie privée. Plus précisément, l'argument portait sur le caractère non accessible et

[623] Voir par exemple en ce sens, Cons. const., 2 mars 2004, n°2044-492 DC.
[624] Cons. const., 22 mars 2012, n°2012-652 DC.
[625] CE, 26 octobre 2011, n°317827, *Association pour la promotion de l'image.*
[626] CE, 10e et 9e sous section réunies, 16 avril 2010, n°320196.

non prévisible de l'ingérence permise par le décret du fait de l'absence de publication. Le Conseil d'Etat a rejeté ses arguments, arguant de la nécessité et de la proportionnalité de la mesure. Cette dernière étant de plus assortie de garanties suffisantes[627].

223. L'exemple du contrôle de légalité du TAJ – Le Conseil d'Etat s'est également prononcé sur la légalité du fichier de traitement des antécédents judiciaires (TAJ). Malgré le développement de nouvelles garanties, des craintes subsistent quant au bon fonctionnement du fichier. Outre les questions précédemment abordées d'erreurs de saisie présentes dans le fichier du fait de la récupération des données des STIC et JUDEX, plusieurs points sont d'ores et déjà critiqués. Cinq arguments étaient invoqués par la Ligue des droits de l'Homme à l'appui de ses prétentions. Dans un premier temps la Ligue des droits de l'Homme invoquait une atteinte à la présomption d'innocence[628] en raison de l'inscription au fichier des personnes avant même toute condamnation définitive. Cet argument a été rejeté par le Conseil d'Etat qui a considéré que le principe d'effacement des données en cas de classement sans suite, relaxe, non-lieu ou acquittement suffisait à prévenir toute atteinte au principe. Aussi, le requérant invoquait une atteinte au principe du droit au respect de la vie privée[629] causée par l'enregistrement de photographies en vue de la mise en œuvre du dispositif de reconnaissance faciale. Le Conseil d'Etat a considéré que le stockage de ces données répondait à un intérêt général et ne portait pas une atteinte excessive à la protection de la vie privée. Les juges ont estimé que le fichage des photographies est utile et répond à des « finalités légitimes ». En outre, le Conseil d'Etat juge que le décret portant création du TAJ apporte des garanties suffisantes. Sur la question soulevée des durées excessives de conservation des données, le Conseil d'Etat a considéré que les durées appliquées étaient fonction de la gravité des faits incriminés et qu'elles étaient nécessaires et justifiées au vu des finalités du fichier. Par ailleurs, les juges ont estimé que la liste des personnes habilitées à consulter le fichier ne porte pas atteinte aux libertés individuelles et mentionnent qu' *« aucune norme constitutionnelle ne s'oppose, par principe, à l'utilisation à des fins administratives de données nominativement recueillies dans le cadre d'activités de police judiciaire »*. Le Conseil d'Etat a donc le 11 avril 2014[630] rejeté les arguments invoqués par le demandeur et conclu à la légalité du décret du 4

[627] Voir à ce sujet, V. Gautron, Fichiers de police, réglementation française, *op. cit.*, p. 54-57. Le Conseil d'Etat rejette la demande d'annulation des décrets relatifs au fichier CRISTINA, *JCP G*, n°17, 26 avril 2010, 480.
[628] Le principe de présomption d'innocence est garanti par l'article 6 de la Convention européenne des droits de l'homme et l'article 6 de la Déclaration des droits de l'homme et du citoyen.
[629] Le principe du droit au respect de la vie privée est garanti par l'article 8 de la Convention européenne des droits de l'homme.
[630] CE, 10e et 9e sous section réunies, 11 avril 2014, n° 360759.

mai 2012[631] se fondant une fois de plus sur la proportionnalité des atteintes au vu de la finalité du fichier.

224. Un contrôle de légalité portant rarement annulation de l'acte créant le fichier – Le Conseil d'Etat n'a prononcé l'annulation totale d'un acte règlementaire qu'une seule fois. Il s'agissait d'apprécier la légalité du fichier ELOI (pour éloignement des irréguliers) créé par arrêté ministériel du 30 juin 2006[632]. Le but de ce fichier est de lutter contre l'immigration clandestine et favoriser l'éloignement des personnes en situation irrégulière. Pour ce faire, il prévoyait l'enregistrement des empreintes digitales et d'une photographie des étrangers sollicitant la délivrance d'un titre de séjour, ou de personnes en situation irrégulière faisant l'objet d'une mesure d'éloignement ou ayant été contrôlées à la frontière et ne remplissant pas les conditions d'entrée sur le territoire. Saisi par le groupement d'information et de soutien aux immigrés (GISTI) et plusieurs associations dont SOS racisme, le Conseil d'Etat, dans une décision du 12 mars 2007[633], avait jugé qu'au regard de la nature des informations contenues dans le fichier, seul un décret pouvait fixer les modalités du fichage. Le Conseil d'Etat a donc prononcé la nullité totale du fichier en se fondant sur l'incompétence de son auteur. Après avis de la CNIL[634] le gouvernement adopte par le décret du 26 décembre 2007[635] le nouveau fichier ELOI. Cette nouvelle version fut également dénoncée par plusieurs associations[636] notamment la disposition qui tendait à intégrer au fichier ELOI le numéro dit « AGDREF [637]» plus précisément le numéro attribué par les services de préfecture lors des demandes de titre de séjour. Le Conseil d'Etat dans sa décision du 30 décembre 2009[638]a invalidé partiellement le nouveau dispositif. ~~L~~es requérants invoquaient le fait que la finalité statistique du fichier n'était pas suffisamment encadrée, que les données collectées ne présentaient un caractère ni adéquat ni pertinent au vu de ses finalités, que les durées de conservations prévues pour certaines données étaient trop longues et enfin que le nombre de destinataires du fichier était trop important. Le Conseil d'Etat a retenu deux illégalités. En effet, il retient que

[631] Voir par exemple, E. Allain, Légalité du nouveau fichier de police (TAJ) : le volet pénal, *Dalloz actualité*, 16 avril 2014.
[632] Le fichier Eloi est créé en application de l'article L.611-3 du C.E.S.E.D.A.
[633] CE 12 mars 2007, *Gisti et autres*, n°297888.
[634] Délibération CNIL n°2007-110 du 24 mai 2007 portant avis sur un projet de décret pris pour l'application du deuxième alinéa de l'article L. 611-3 du code de l'entrée et du séjour des étrangers et du droit d'asile portant création d'un traitement automatisé de données à caractère personnel des ressortissants étrangers faisant l'objet d'une mesure d'éloignement et modifiant la partie réglementaire de ce même code.
[635] Décret n°2007-1890 du 26 décembre 2007 créant le fichier ELOI.
[636] Notamment, le groupement d'information et de soutien aux immigrés (GISTI), la ligue des droits de l'homme (LDH), SOS racisme, Cimade et Imaginons un réseau internet solidaire (Iris).
[637] Pour Application générale des ressortissants étrangers en France.
[638] CE 30 décembre 2009, *SOS racisme, Gisti et a.*, n°312051 et n°313760.

l'enregistrement du numéro AGDREF dans le fichier ELOI n'est ni adéquat ni pertinent au vu des finalités et estime que la durée de conservation de trois ans concernant les données relatives à l'identification et aux mesures d'éloignement était excessive.
Finalement, le juge de l'excès de pouvoir n'hésite pas à sanctionner des dispositifs qui reposent sur des données dont le fichage manque de pertinence ou d'adéquation avec la finalité du fichier, néanmoins, il s'agit le plus souvent d'une nullité partielle[639]. Le contrôle de constitutionnalité s'avère souvent plus sévère.

§3. Le contrôle de constitutionnalité

225. Contrôle de constitutionnalité – Les normes et principes édictés par la Constitution trouvent nécessairement à s'appliquer en matière de fichiers judiciaires. Le rôle du Conseil constitutionnel réside principalement dans le contrôle de la conformité des lois à la Constitution[640]. Avant 2010, ce contrôle était limité puisqu'il nécessitait la saisine a priori par les autorités compétentes. Depuis la révision constitutionnelle du 23 juillet 2008[641], le Conseil constitutionnel peut être saisi par tout justiciable en cours d'instance dès lors qu'il soulève la non-conformité d'une loi à la Constitution.
S'agissant de la création de fichiers judiciaires, il convient de s'intéresser au contrôle effectué à priori sur les lois portant création d'un fichier (A.). Néanmoins, ce contrôle peut également se faire a posteriori par le biais de question prioritaire de constitutionnalité (B.).

A. Le contrôle a priori des lois portant création de fichiers judiciaires

226. A priori – Le Conseil constitutionnel a eu à se prononcer sur la question de la conformité de lois portant création de fichiers de police par le biais d'un contrôle a priori. Il opère ainsi un contrôle de proportionnalité qui est d'autant plus affirmé depuis sa décision du 22 mars 2012 dans laquelle il a jugé que le droit au respect de la vie privée implique que « la collecte, l'enregistrement, la conservation, la consultation et la communication de données à caractère personnel justifiés par un motif d'intérêt général soient mis en œuvre de manière adéquate et proportionnée à cet objectif » [642]. Plusieurs fichiers ont fait l'objet de ce contrôle a priori. En

[639] G.. Begranger, Le contrôle des fichiers de police par les juges, *op. cit.*
[640] Art. 61 et 61-1 de la Constitution.
[641] Insérant l'article 61-1 dans la Constitution, entré en vigueur au 1er mars 2010.
[642] Cons. const. n°2012-652 DC du 22 mars 2012.

matière de fichiers de police, sont invoquées des atteintes au droit au respect de la vie privée, au principe de dignité, à la présomption d'innocence ou encore au secret des correspondances.

1° Validation par le Conseil constitutionnel

227. L'exemple du contrôle *a priori* du STIC et JUDEX – Le Conseil constitutionnel s'est prononcé sur la conformité des fichiers d'antécédents judiciaires (à l'époque du STIC et du JUDEX) dans le cadre du contrôle opéré sur la loi dite « LOPPSI II » du 14 mars 2011. Dans une décision du 10 mars 2011[643], il a considéré que les dispositions de la loi en question relatives aux fichiers d'antécédents avaient pour effet de « renforcer le contrôle de l'autorité judiciaire sur les données enregistrées dans les fichiers d'antécédents ». Il a donc validé les dispositions sous réserve toutefois de respect des garanties déjà évoquées dans sa décision du 13 mars 2003[644]. Ainsi, il rappelle que les données fichées ne peuvent servir dans le seul cadre de décisions administratives, ni intervenir en matière de demande de titre de séjour ou d'obtention de la nationalité française.

Une partie de la doctrine soulève néanmoins la question de la disparition de la frontière entre administratif et judiciaire qui rend difficile la conservation de cette distinction stricte et met à mal le principe de finalité. La CNIL a également dénoncé certaines pratiques notamment dans son rapport de 2008. Ces pratiques peuvent par exemple ouvrir l'accès de fichiers de police à la police administrative. S'éloignant alors du principe de finalité initiale ces pratiques sont parfois validées par le Conseil constitutionnel au nom du principe de nécessité et sous couvert du respect du principe de proportionnalité[645].

[643] Cons. const. n°2011-265 DC du 10 mars 2011relative à la loi du 14 mars 2011 qui codifie aux articles 230-6 à 230-11 du code de procédure pénale en apportant des modifications les dispositions de l'article 21 de la loi du 18 mars 2003. Les requérants se fondaient principalement sur les recommandations de la CNIL dans son rapport du 20 janvier 2009 et invoquaient le non respect du principe issu de la loi informatique et libertés de 1978 en fonction duquel les données faisant l'objet d'un traitement doivent être exactes et mises à jour. Il n'appartenait donc pas au Conseil constitutionnel de juger de la conformité des dispositions litigieuses à la Loi informatique et libertés. Il faut noter que lors de ce contrôle certaines dispositions de la loi ont été censurées par le Conseil constitutionnel.

[644] Cons. const. n°2003-467 DC du 13 mars 2003 relative à la loi pour la sécurité intérieure.

[645] Cela a été le cas par exemple concernant l'accès de l'Administration à certains fichiers tels que le STIC dans le cadre des enquêtes de moralité effectuées avant l'accès à certaines professions dites « sensibles ». L'article L. 114-1 du code de la sécurité intérieure consacre de telles pratiques.
Le Conseil constitutionnel juge cette consultation nécessaire notamment dans sa décision du 13 mars 2003 précitée.
Cette pratique a été entérinée par décret n°2005-1124 du 6 septembre 2005 qui dresse la liste des professions pour lesquelles une telle enquête est possible.

228. L'exemple du contrôle *a priori* du FIJAIS – Un contrôle de conformité a également été opéré sur la loi instituant le FIJAIS. Les requérants invoquaient une atteinte au principe de nécessité des peines et au droit au respect de la vie privée ainsi qu'au principe fondamental reconnu par les lois de la République en matière de droit pénal des mineurs. Par une décision du 2 mars 2004[646], le Conseil constitutionnel a jugé que l'inscription au fichier a pour vocation « *de prévenir le renouvellement de ces infractions et de faciliter l'identification de leurs auteurs ; qu'il en résulte que cette inscription ne constitue pas une sanction mais une mesure de police* ». Ainsi, le Conseil constitutionnel a validé le dispositif.

229. L'exemple du contrôle *a priori* de la loi relative à la rétention de sureté – Le Conseil constitutionnel a également dû se prononcer sur la loi du 25 février 2008[647] relative à la rétention de sûreté. Cette dernière prévoyait l'inscription au bulletin n°1 et n°2 des décisions d'irresponsabilité pénale[648]. Les requérants invoquaient une atteinte grave au droit au respect de la vie privée. Le conseil a admit que cette inscription portait atteinte aux libertés individuelles. Il a néanmoins validé le dispositif sous réserve que l'inscription soit assortie de garanties. Plus précisément, l'inscription sera effectuée lorsque la décision sera assortie de mesures telles que l'admission en centre de soin[649].

2° Censure du Conseil constitutionnel

230. La censure pour incompétence négative – Si le Conseil constitutionnel ne s'est pas prononcé sur la conformité de la loi informatique et libertés de 1978, il a eu à examiner la loi du 6 août 2004[650] la modifiant. Pour la première fois en matière de fichiers, le Conseil censure partiellement une loi pour incompétence négative c'est-à-dire qu'il reproche au législateur d'avoir délégué une compétence qu'il devrait lui-même exercer[651]. Dans sa décision du 29

[646] Cons. const., n°2004-492 DC du 2 mars 2004.
[647] Loi n°2008-174 du 25 février 2008 relative à la rétention de sûreté et à la déclaration d'irresponsabilité pour cause de trouble mental.
[648] Ces dispositions sont prévues par l'article 4 de la loi déférée et codifiées aux articles 768, 775 et 706-135 du code de procédure pénale.
[649] V. l'article 706-135 du code de procédure pénale.
[650] 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.
[651] Plus particulièrement, le Conseil constitutionnel reproche au législateur l'alinéa 3 de l'article 9 de la loi qui prévoyait qu'une personne morale s'estimant victime d'une infraction pénale de pouvoir mandater d'autres personnes morales pour recueillir des informations nominatives portant sur les infractions ou les condamnations.

juillet 2004[652], le conseil a censuré ce dispositif considérant que le traitement de données personnelles qui en découlerait pourrait affecter le droit au respect de la vie privée des individus. De plus, il a considéré que la loi était trop imprécise et ambigüe sur la question notamment de l'étendue du *mandat* visé.

231. La censure pour atteinte à un droit fondamental garanti par la Constitution – Bien que ne visant pas directement un fichier judiciaire, il convient de citer la décision du conseil en date du 22 mars 2012[653] par laquelle ce dernier a censuré les dispositions de la loi relative à la protection de l'identité qui prévoyait la création d'un fichier central biométrique à dimension nationale rassemblant les données de toutes les cartes d'identité et passeports des individus. Au regard de l'ampleur du fichage qui visait l'ensemble de la population et aux risques de dérives, le conseil a considéré que la création du fichier portait une atteinte excessive au droit au respect de la vie privée. Les sages ont également fait référence à la nature « sensible »[654] des données concernées pour appuyer leur décision.

B. Le contrôle a posteriori des lois portant création de fichiers de police

232. A posteriori – Aux termes de l'article 61-1 de la Constitution, tout justiciable peut, à l'occasion d'une instance en cours, soulever la non-conformité d'une loi, applicable à son litige, aux droits et libertés que la Constitution garantit par le biais d'une question prioritaire de constitutionnalité (QPC). La disposition législative contestée doit être applicable au litige ou constituer le fondement des poursuites et ne pas être dépourvue d'un caractère sérieux. Aussi, cette dernière ne doit pas avoir été déclarée conforme à la Constitution.

233. Application en matière de création de fichiers – Concrètement, en matière de fichiers, ce dispositif concerne les lois portant création d'un fichier judiciaire n'ayant pas déjà fait l'objet d'un contrôle de constitutionnalité a priori. Néanmoins on peut envisager le dépôt d'une QPC s'agissant d'une loi nouvelle qui viendrait étendre la finalité d'un fichier.
Finalement, une seule question prioritaire de constitutionnalité a été posée en matière de fichier judiciaire. Cette dernière était relative au FNAEG. Par décision du 16 septembre

[652] Cons. const. n°2004-499 DC du 29 juillet 2004.
[653] Cons. const. n°2012-652 DC du 22 mars 2012.
[654] Il convient de noter que la notion de donnée « sensible » est entendue très largement par le Conseil constitutionnel.

2010[655], le conseil constitutionnel a validé le dispositif. Toutefois, il a émis quelques réserves. Ainsi, la liste des infractions permettant l'inscription au fichier doit être « strictement limitée » et la durée de conservation des données doit être fixée par décret et être proportionnelle à « la nature ou à la gravité des infractions concernées ». Cette décision fait suite à l'arrêt de la Cour européenne des droits de l'homme du 4 décembre 2008 *S. et Marper c. Royaume-Uni*[656] dans lequel les juges ont considéré que la conservation pour une durée illimitée de données relatives à des personnes non condamnées constitue une atteinte au droit au respect de la vie privée.

Ces différentes décisions n'ont toutefois pas entraîné l'adoption d'un décret visant à mieux encadrer les durées de conservation des données. Plusieurs institutions et organismes continuent à alerter sur certains risques de dérives liées au développement de ce fichier. Dans un communiqué commun du 21 novembre 2011, le syndicat de la Magistrature, le syndicat des avocats de France et la Ligue des droits de l'Homme ont exprimé leurs inquiétudes concernant les évolutions du fichier relevant notamment « l'expansion » du nombre de personnes visées par le fichage et l'augmentation des infractions permettant l'inscription. Rappelant les différentes décisions du Conseil constitutionnel et de la CEDH, ces derniers ont aussi critiqué les durées de conservation des données « manifestement disproportionnées ». Les rédacteurs du communiqué craignent également les dérives d'un tel fichage au vu du développement et des progrès de la génétique. De telles données pourraient permettre d'identifier l'origine géographique de la personne ainsi que d'éventuelles pathologies par exemple. Ils demandent alors que seules les personnes condamnées puissent être fichées, que le nombre d'infractions permettant l'inscription soit réduit, que les durées de conservation soient plus strictement encadrées (notamment concernant les mineurs) et que la réhabilitation emporte automatiquement effacement au fichier[657].

234. Contrôle par le biais de la QPC – Le mécanisme de la question prioritaire de constitutionnalité est peu utilisé jusqu'à présent en matière de fichiers de police. Il faut toutefois rappeler que le système de double filtre[658] peut bloquer la transmission d'une

[655] QPC n°2010-25 16 sept. 2010.Voir à ce sujet, Les cahiers du Conseil constitutionnel, n°30. Saisi le 17 juin 2010 par la Cour de cassation, arrêt n°12071 du 11 juin 2010.
[656] CEDH, 4 décembre 2008, *S. et Marper c/ Royaume-Uni*,
[657] Communiqué commun Syndicat de la Magistrature, Syndicat des avocats de France, LDH, 21 novembre 2011.
[658] Le mécanisme de double filtre réside dans l'appréciation faire par le juge saisi du litige de l'opportunité ou non de transmettre la question au juge suprême dont il dépend. Ce dernier opérant à son tour un contrôle et une appréciation sur la question transmet au Conseil constitutionnel qui appréciera à son tour le bien fondé de la

question au Conseil constitutionnel. Par exemple, dans l'arrêt du 19 juin 2012[659] la cour de cassation a eu à se prononcer sur la transmission d'une question prioritaire de constitutionnalité portant sur la conformité des dispositions des articles 706-54 et 706-56 III du code de procédure pénale relatifs aux prélèvements biologiques et au fichage de données génétiques dans le FNAEG. La chambre criminelle de la Cour de cassation a jugé que la question soulevée avait déjà fait l'objet d'une décision. Plus précisément, dans une décision du 16 septembre 2010, le Conseil constitutionnel a prononcé la conformité des dispositions. La question prioritaire de constitutionnalité n'a donc pas été renvoyée devant le Conseil constitutionnel.

Le Conseil d'Etat s'est également prononcé sur la transmission d'une QPC relative au traitement de données personnelles dans une décision du 12 mai 2011[660]. Le requérant invoquait la non-conformité de certaines dispositions de la loi informatique et libertés du 6 janvier 1978 à la Constitution[661] (notamment aux articles 1 et 34 de la Constitution[662]). Le Conseil d'Etat décide de ne pas transmettre la QPC pour plusieurs motifs. Les juges vont

---

question et s'il y a lieu à statuer. Pour ces raisons, une partie de la doctrine fait référence à un triple filtre. Voir en ce sens, A. Roblet-Troizier *in Les nouveaux cahiers du Conseil constitutionnel*, n°40, 2013.

[659] Cass. crim., 19 juin 2012, *pourvoi* n°12-90022, *inédit*. Saisie lors d'un jugement correctionnel du chef de refus de se soumettre à un prélèvement biologique, le Conseil constitutionnel a eu à répondre à la question suivante : *«Les dispositions de l'avant dernier alinéa de l'article 706-54 du code de procédure pénale sont-elles conformes au principe constitutionnel de sauvegarde de la dignité humaine protégé par le préambule de la Constitution du 27 octobre 1946 et au principe constitutionnel de respect de la vie privée protégé par l'article 2 de la Déclaration des droits de l'homme et du citoyen de 1789 ? Les dispositions prévues par l'article 70656 III du code de procédure pénale et relatives au retrait et à l'octroi, de plein droit, de réductions de peine, en cas de condamnation pour refus par une personne condamnée de se soumettre au prélèvement biologique destiné à l'identification de son empreinte génétique, portent-elles atteinte à l'article 66 de la Constitution (privation de liberté sans l'intervention de l'autorité judiciaire) et aux articles 8 et 16 de la Déclaration des droits de l'homme et du citoyen de 1789 (principe de nécessité des peines, principe du droit au recours à un juge) ? Les dispositions de I 'article 706-54 telles que modifiées successivement par la loi n° 2010242 du 10 mars 2010 (art.19) et la loi n° 2011267 du 14 mars 2011 (art.9) portent-elles atteinte à l'article 2 de la Déclaration des droits de l'homme et du citoyen de 1789 (respect de la vie privée) et au principe constitutionnel de sauvegarde de la dignité humaine protégé par le préambule de la Constitution du 27 octobre 1946 ? Les dispositions de l'article 70656 telles que modifiées successivement par la loi n° 2010242 du 10 mars 2010 (art. 19) et la loi n° 2011267 du 14 mars 2011 (art.9) portent-elles atteinte à l'article 2 de la Déclaration des droits de l'homme et du citoyen de 1789 (respect de la vie privée) et au principe constitutionnel de sauvegarde de la dignité humaine protégé par le préambule de la Constitution du 27 octobre 1946 ? »*

Voir aussi, Cass. crim. 11 juillet 2012, *pourvoi* n°12-81533, *inédit.*

[660] CE. 12 mai 2011, n°318952, *inédit.*

[661] La question prioritaire a été soulevée à l'occasion d'une instance portant sur une demande de nullité de plusieurs décrets instituant notamment le fichier EDVIGE utilisé par les services de renseignements généraux. Le requérant soulève la non-conformité des articles 6, 8, 25, 26, 27, 30, 40, 41 et 42 de la loi n° 7817 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

[662] L'article 1er de la Constitution du 4 octobre 1958 pose les principes d'une République indivisible, laïque, démocratique et sociale. L'article 34 est relatif au cadre législatif et au domaine de la loi.

considérer que certaines des dispositions contestées ne sont pas applicables au litige[663], que certaines ont été déjà jugées comme conformes[664] et enfin que s'agissant des autres dispositions litigieuses la question n'est ni nouvelle ni sérieuse[665]. Là encore, les juges ont décidé de ne pas transmettre la question prioritaire de constitutionnalité portant sur la conformité de dispositions relatives à un fichier judiciaire.

235. Constat – Finalement, le Conseil constitutionnel a validé la quasi-totalité des fichiers de police qui ont été soumis à son appréciation et à son contrôle que ce soit par saisine a priori ou par le biais d'une question prioritaire de constitutionnalité. Les sages préfèrent souvent valider un dispositif et l'assortir de garanties sous forme de réserves plutôt que de censurer totalement une loi ou un projet de loi qui lui est soumis[666].

Ce contrôle sur les fichiers s'opère également au niveau supra national.

§4. Le contrôle des juges supranationaux

236. L'intérêt nécessaire des juges supra nationaux pour les fichiers – La jurisprudence en la matière confirme l'intérêt porté par les juges supra nationaux sur la question du fichage. Il est désormais acquis pour la Cour européenne des droits de l'Homme que le fichage de données à caractère personnel lors d'une procédure judiciaire constitue une ingérence dans le droit au respect de la vie privée[667]. La Cour européenne des droits de l'Homme a depuis longtemps adopté une définition large de la notion de vie privée[668] considérant qu'il est impossible d'en poser une définition exhaustive ; c'est donc en toute logique qu'elle a admis que le fichage de données personnelles entrait dans le champ d'application de l'article 8. En effet, les données à caractère personnel en ce qu'elles constituent des données attachées à l'identité, peuvent lors de leur traitement porter une atteinte à la vie privée permettant l'identification des individus.

Par exemple dans l'arrêt du 4 mai 2000[669], la Cour européenne des droits de l'Homme rappelle que *« la collecte, la mémorisation et la communication de données relatives à la vie privée entrent dans le champ d'application de l'article 8* ». Aussi, dans l'arrêt du 28 janvier

[663] Il s'agit des articles 25 et 27 de la loi de 1978.
[664] Il s'agit des articles 8 et 26 de la loi de 1978 jugées conforme à la Constitution dans la décision n°2004-99 DC du 29 juillet 2004.
[665] S'agissant des articles 6, 30, 40, 41 et 42 de la loi de 1978.
[666] Voir à ce sujet, G.. BEGRANGER, Le contrôle des fichiers de police par les juges, *op. cit.*
[667] C.E.D.H., 4 décembre 2008, *S. et Marper c/ Royaume-Uni*.
[668] Voir par exemple CEDH, 29 avril 2002, *Prety c/ Royaume-Uni.*
[669] C.E.D.H., 4 mai 2000, *Rotaru c/ Roumanie.*

2003 *Peck c/ Royaume-Uni,* la Cour européenne des droits de l'Homme a jugé que l'enregistrement par le biais de systèmes de vidéo surveillance de films pouvait entrer dans le champ d'application de l'article 8.
La Cour européenne des droits de l'Homme a aussi précisé que les données publiques pouvaient entrer dans le champ d'application de l'article 8[670].

237. Contrôle de conventionalité du FIJAIS – La Cour européenne des droits de l'Homme a eu à se prononcer sur la conventionalité du FIJAIS dans un arrêt du 17 décembre 2009 *M.B. c/ France*[671]. La question était soulevée de l'inscription au fichier créé en 2004 de condamnations antérieures. La méconnaissance de l'article 7[672] a été écartée. Toutefois, cette interrogation a permis de préciser la nature même du fichier. La CEDH a considéré que ce dernier ne constitue pas une peine mais une « mesure préventive » s'alignant ainsi sur le point de vue du Conseil constitutionnel dans sa décision du 2 mars 2004. Ce dernier faisait alors référence à une « mesure de police ». Bien que n'ayant pas été saisie de la question, la Cour a examiné la conformité du dispositif à l'article 8 et en a conclu l'existence d'une ingérence dans la vie privée des individus fichés, ingérence néanmoins « légitime ». Elle a considéré que les politiques pénales sont aujourd'hui soucieuses de s'assurer de la réinsertion des individus condamnés et « qu'une réinsertion réussie présume notamment la prévention de la récidive ». Aussi, bien que les données puissent être conservées 30 ans, le droit d'effacement suffit à garantir le droit au respect de la vie privée[673].
Finalement s'il est admis que le fichage de données par les autorités judiciaires peut porter une atteinte excessive aux droits et libertés garanties par la convention, la Cour européenne des droits de l'Homme opère d'avantage un contrôle de proportionnalité sur l'utilisation et la gestion des fichiers que sur leur création même.
Au-delà des interrogations relatives à la création des fichiers de police, se posent celles liées au partage des données fichées. La question de l'utilisation fait des données fichées interroge d'autant plus que celles-ci peuvent faire l'objet d'une communication parfois automatique. Ce partage renvoie aux mécanismes de rapprochement ou d'interconnexion mais au delà soulève la question du transfert hors des frontières parle biais de la coopération internationale.

[670] Voir par exemple, CEDH, 16 février 2000 *Amann c/ Suisse.*
[671] C.E.D.H., 17 décembre 2009, *B.;G.;M.B. c/ France*.
[672] Convention européenne des droits de l'Homme et du citoyen, article 7 « pas de peine sans loi ».
[673] Voir à ce sujet, N. Hervieu, « Conventionalité de l'inscription au FIJAIS », *Combats pour les droits de l'homme*, 22 décembre 2009.

CHAPITRE 2 : LE PARTAGE DE DONNEES FICHEES

238. Rapprochement et interconnexion – Il convient d'abord de distinguer le simple rapprochement de données de l'interconnexion. Ainsi, le rapprochement de données ne suppose pas nécessairement une automatisation et peut s'effectuer au sein d'un même fichier alors que l'interconnexion est un mécanisme automatique qui peut permettre la mise en relation de données issues de fichiers différents[674]. Plus précisément, l'interconnexion vise *« tout traitement automatisé mis en œuvre par un ou plusieurs responsables qui consiste à mettre en relation (corréler) des données ayant une finalité avec d'autres données ayant une finalité identique ou différente. Cette mise en relation (ou corrélation) peut consister à transférer un fichier pour alimenter un autre fichier ou pour réaliser la fusion de ces fichiers, à mettre ponctuellement en relation plusieurs fichiers normalement gérés séparément, par exemple en constituant un fichier d'appel à partir de l'un de ces fichiers qui servira à interroger les autres fichiers et sera enrichi par les résultats de cette consultation. Il peut également s'agir d'assembler des informations provenant de plusieurs fichiers au sein d'une même base de données (exemple des bases dénommées « entrepôts de données » alimentés par des informations provenant de différents fichiers) avec un éventuel recours à des techniques logicielles de mises en relations ponctuelles (outils dits de datamining) ou de créer un lien technique entre plusieurs bases de données nominatives qui permettra, par exemple, de les consulter simultanément (par exemple, des sites portails permettant par des « liens hypertextes » d'assurer une mise en relation avec d'autres bases)»*[675]. La CNIL retient trois critères cumulatifs permettant de définir la notion d'interconnexion. Tout d'abord, il s'agit de mettre en relation des fichiers contenant des données à caractère personnel. Ensuite, ce mécanisme doit porter sur au moins deux fichiers distincts. Enfin, le mécanisme doit être automatisé.

239. Contrôle de la CNIL sur toute interconnexion de fichiers – La CNIL va de manière générale s'assurer que toute interconnexion de fichiers est justifiée et assortie de garanties suffisantes. C'est le cas par exemple, s'agissant de l'ACCReD créé par décrets en date du 3

[674] Voir les notions telles que définies par la CNIL, « *Comment déterminer la notion d'interconnexion ?* », 5 avril
2011, https://www.cnil.fr/en/node/15316.
[675] Voir le glossaire édité par le CNRS.

août 2017[676]. Ce fichier a pour finalité de faciliter les enquêtes administratives réalisées au sujet d'individus ayant accès aux centrales nucléaires intéressant la défense nationale ou ouvrages d'importance vitale. Le fichier opère une consultation automatique de différents autres fichiers tels que le TAJ, le FPR, la PASP, le GIPASP ou CRISTINA. Le décret du 3 août 2017 a donc permis d'étendre l'accès à plusieurs fichiers en matière d'enquêtes administrative. Initialement ces fichiers ne faisaient l'objet d'aucune interconnexion. Dans sa délibération du 9 décembre 2010 relative au projet de décret portant création du GIPASP, la CNIL s'était intéressée à la question de l'interconnexion du fichier qui n'était alors pas envisagée dans les textes. Néanmoins, la Commission avait formulé plusieurs remarques à ce sujet. Les dispositions du code de la sécurité intérieure prévoyant l'enregistrement de données relatives à « des agissements susceptibles de recevoir une qualification pénale », la Commission semblait craindre un rapprochement ou une interconnexion avec d'autres fichiers tels que le STIC ou le JUDEX. Aussi, la CNIL mentionnait l'existence d'une consultation simplifiée du fichier par l'intermédiaire d'un autre traitement (Gestion des sollicitations et interventions GSI) à partir de l'identité de la personne. Dans la délibération, la CNIL alertait sur le fait qu'un tel dispositif pouvait constituer une interconnexion telle que définie par la loi informatique et libertés. Le décret du 3 août 2017 est venu modifier les dispositions relatives à plusieurs fichiers et permet désormais clairement une interconnexion entre plusieurs d'entres eux. La CNIL dans son avis relatif au projet de décret a considéré que ses dispositions découlent des évolutions du code de la sécurité publique et du renforcement des contrôles, justifiant ainsi la mise en œuvre d'interconnexions[677].

240. Interrogations soulevées par les mécanismes de rapprochement et d'interconnexion – La loi informatique et libertés distingue le rapprochement de données et l'interconnexion notamment dans son article 33[678]. L'article 2 de la Directive du 24 octobre 1995 opérait la même distinction dans sa définition du traitement de données[679]. Plus récemment, le

[676] Décret n° 2017-1224 du 3 août 2017 portant création d'un traitement automatisé de données à caractère personnel dénommé « Automatisation de la consultation centralisée de renseignements et de données » (ACCReD).

[677] Délibération n°2017-153 du 18 mai 2017 portant avis sur un projet de décret modifiant plusieurs traitements automatisés de données à caractère personnel du code de la sécurité intérieure.

[678] Art. 33 de la LIL *« I.-Les demandes d'avis adressées à la Commission nationale de l'informatique et des libertés en vertu de la présente loi précisent : […]*

3° Le cas échéant, les interconnexions, les rapprochements ou toutes autres formes de mise en relation avec d'autres traitements ; »

[679] Art. 2 de la Directive du 24 octobre 1995 *« Aux fins de la présente directive, on entend par: b) « traitement de données à caractère personnel » (traitement): toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel, telles que la collecte,*

règlement européen sur la protection des données[680] reprend la même définition du traitement de données distinguant le rapprochement de l'interconnexion. On devine immédiatement les interrogations et les craintes soulevées par cette pratique, que certains qualifient d'interopérabilité[681], notamment lorsqu'il s'agit de données sensibles et plus particulièrement de données issues de fichiers de police. L'interconnexion automatisée peut par définition mettre en corrélation des fichiers ayant initialement une finalité différente et donc mettre à mal le principe de base du traitement de données à caractère personnel fixé par la loi informatique et libertés qui dispose qu'un traitement doit être mis en œuvre pour une finalité déterminée. C'est ainsi, par exemple, que les données de fichiers administratifs et judiciaires se trouvent interconnectées. Cette interconnexion permet également d'alimenter les fichiers à partir d'autres fichiers ce qui explique la reprise de données erronées qui a pu être constatée dans certains d'entre eux. Face aux risques liés à l'interconnexion de fichiers, la loi informatique et libertés a soumet l'interconnexion de fichiers ayant des finalités différentes à un régime d'avis préalable par la CNIL, autrefois soumis au régime d'autorisation[682]. Qu'il s'agisse d'interconnexions ou de simples rapprochements de données, des questions relatives à l'encadrement de ces mécanismes et à la protection des données trouvent nécessairement à se poser[683]. Il convient de distinguer les transferts de données opérés au niveau national (Sect. 1) de ceux opérés au niveau international (Sect. 2).

Section 1 : Le partage de données à caractère personnel au niveau national

241. Transferts nationaux – Dans le cadre des procédures judiciaires, les données fichées peuvent faire l'objet de différents transferts. Il peut s'agir de simples rapprochements de données réalisés sur demande d'une autorité et dans le cadre d'une procédure particulière (§1) ou bien d'interconnexions ou mises en relation automatiques de données issues de fichiers distincts (§2).

---

l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction ».

[680] Règlement (UE) 2016/679 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).

[681] Voir par exemple, JJ. Lavenue, « L'interopérabilité et l'interconnexion des fichiers de police : enjeux et ambiguïté du rapport dialectique entre principe d'efficacité et protection des libertés », *Institut du monde et du développement pour la bonne gouvernance publique IMODEV,* vol. 1, 2014.
Rapport du groupe de diagnostic stratégique n°6, 25e session nationale « Sécurité et Justice », 2013/2014, « Fichiers de police et libertés : des enjeux nationaux, une nouvelle donne internationale », janvier 2015.

[682] Article 33 de la loi informatique et libertés. L'ancien article 25 de la LIL prévoyait le régie d'autorisation.

[683] Les questions relatives à la protection des données seront abordées dans la seconde partie.

§1. Le rapprochement de données judiciaires

242. Rapprochement au niveau national – Le rapprochement de données vise toute action de l'homme effectuée dans le but de mettre en corrélation ou de confronter différentes données au sein d'un même fichier ou issues de fichiers différents. Cette manipulation n'est donc pas automatique et il s'agit d'interroger un fichier. Cette demande peut intervenir à l'initiative de différents acteurs notamment pendant la phase d'enquête. Il ne s'agira pas ici de recenser toutes les personnes ayant un droit d'accès aux fichiers de police, mais de s'interroger sur les outils permettant un tel rapprochement. Il s'agit dans un premier temps des outils d'analyse sérielle (A), puis dans un second temps des logiciels de rapprochement (B).

A. Les outils d'analyse sérielle

243. L'analyse sérielle – La loi LOPPSI 2 du 14 mars 2011[684] a introduit dans le code de procédure pénale la possibilité pour les services de police et de gendarmerie de *« mettre en œuvre des traitements automatisés de données à caractère personnel »*[685] dans le but de recueillir des preuves et constater des infractions. Ces données peuvent notamment être recueillies au cours d'enquêtes préliminaires, d'enquêtes de flagrance ou sur commission rogatoire. Aussi, de tels traitements peuvent être utilisés dans le but de faire ressortir des liens entre différents individus, évènements ou infractions[686]. Le décret du 7 mai 2012[687] est venu encadrer la mise en œuvre et l'utilisation de tels traitements d'analyse sérielle et de rapprochement judiciaire. Ces traitements peuvent viser des données sensibles au sens de l'article 6 de la loi informatique et libertés de 1978 sous réserve d'être strictement *« nécessaire aux finalités de recherche criminelle »*[688]. Ils peuvent concerner toute personne sans condition d'âge à l'encontre de laquelle il existe des *« indices graves ou concordants rendant vraisemblable qu'elle ait participé à la commission de l'infraction »*[689]. Une personne

[684] Loi n° 2011-267 du 14 mars 2011, d'orientation et de programmation pour la performance de la sécurité Intérieure.
[685] Art. 11 d) de la loi informatique et libertés. Art. 230-6 et 230-12 du CPP.
[686] Art. 230-12 et suivants et R. 40-35 et suivants du code de procédure pénale.
[687] Décret n° 2012-689 du 7 mai 2012 relatif aux conditions de mise en œuvre des fichiers d'analyse sérielle et des logiciels de rapprochement judiciaire.
[688] Art. 11 de la loi n°2011-267 du 14 mars 2011, d'orientation et de programmation pour la performance de la sécurité Intérieure.
[689] Art. 230-13 du code de procédure pénale.

suspecte peut également faire l'objet du traitement d'analyse sérielle. Le décret prévoit que la mise en œuvre du traitement est placée sous le contrôle d'un magistrat du Parquet[690].

La loi LOPPSI 2 a donc étendu et facilité le développement et l'utilisation des fichiers d'analyse sérielle. Ces derniers existaient néanmoins avant son entrée en vigueur. C'est le cas du système d'analyse des liens de la violence associée aux crimes (SALVAC). S'inspirant d'un logiciel canadien du même nom, la cellule SALVAC a été créée par la loi du 18 mars 2003[691]. Les dispositions de la loi ont été ensuite abrogées par la loi du 14 mars 2011[692] puis codifiées à l'article 230-6 du code de procédure pénale. Cette cellule a été intégrée au sein de l'office central pour la répression des violences aux personnes (OCRVP)[693]. Le système permet aux enquêteurs d'établir des liens entre différentes données collectées dans le cadre de différentes affaires à caractère sériel et ainsi *« faciliter la constatation des crimes et délits portant atteinte aux personnes et présentant un caractère sériel »*[694]. Au 1er janvier 2015, le système a permis le rapprochement de 37 affaires judiciaires concernant 220 victimes[695]. Grand nombre de données y sont conservées pour une durée de quarante ans par les enquêteurs spécialement désignés et affectés à l'OCVRP. En cela, le SALVAC peut être présenté comme un fichier de police, mais son utilisation comme outil d'analyse sérielle de données recueillies lors d'enquêtes distinctes en fait un véritable système de rapprochement de données. Les données collectées sont relatives aux personnes impliquées dans une affaire ainsi qu'au lieu, au mode opératoire. De l'identité, adresse, profession et photographie du suspect aux informations relatives aux victimes ou à toute personne susceptible de fournir des renseignements, le système recense des données très détaillées et peut contenir des données sensibles[696]. La base est alimentée par les enquêteurs à partir d'un questionnaire type[697]. Plus

[690] L'article R. 40-37 du code de procédure pénale prévoit que le magistrat est désigné pour trois ans par le garde des sceaux.

[691] Loi n° 2003-239 du 18 mars 2003 pour la sécurité intérieure, article 21 relatif aux dispositions relatives aux traitements automatisés d'informations.

[692] Loi n°2001-267 du 14 mars 2011, d'orientation et de programmation pour la performance de la sécurité intérieure.

[693] L'office central pour la répression des violences aux personnes dont les missions ont été définies par le décret du 6 mai 2006, agit en matière de lutte contre la criminalité organisée et est rattachée à la direction centrale de la police judiciaire.

[694] Article 1er du décret n° 2009-786 du 23 juin 2009 autorisant la mise en œuvre d'un traitement automatisé de données à caractère personnel dénommé « Système d'analyse des liens de la violence associée aux crimes » modifié par le décret n° 2011-1308 du 14 octobre 2011 remplaçant les références aux articles 21 et 21-1 de la loi n° 2003-239 du 18 mars 2003 pour la sécurité intérieure par les références aux dispositions correspondantes des articles 230-6 et suivants du code de procédure pénale.
Voir à ce sujet, V. Gautron, *« Fichiers de police »*, Répertoire de droit pénal et procédure pénale, *op. cit.*

[695] Archives du Ministère de l'intérieur, J. Beck. « L'OCVRP au cœur des ténèbres – Un logiciel qui a fourni ses preuves », 24 septembre 2015.

[696] L'article 4 du décret n°2009-786 du 23 juin 2009 fixe les données pouvant être collectées par le SALVAC. Ces données sont multiples, il s'agit notamment du nom, surnom, alias, sexe, date et lieu de naissance, adresse, situation familiale, photographie, éléments sur le mode de vie, s'agissant des personnes à l'encontre desquelles il

précisément, le système placé sous l'autorité du ministère de l'intérieur recense des données relatives aux individus visés par l'article 230-13 du code de procédure pénale[698] récoltées dans le cadre d'enquêtes ou dans le cadre de commissions rogatoires réalisées en matière de crimes ou de délits lorsque ces crimes ou délits sont punis de plus de cinq ans d'emprisonnement. Les données sont également collectées en matière de tentatives lorsque celles-ci sont punissables, de disparitions inquiétantes ou de recherche des causes de la mort. A titre d'exemple, le SALVAC a permis en 2013[699] de confondre l'auteur de viols et tentatives de viols commis entre 2008 et 2010 notamment grâce au mode opératoire utilisé.
A noter également que les données du SALVAC peuvent faire l'objet de transmissions dans le cadre de la coopération internationale mais qu'il n'existe toutefois aucune interconnexion entre les fichiers des différents Etats[700].

244. Bases d'analyse sérielle de police judiciaire – En matière d'analyse sérielle, le décret du 22 novembre 2013[701] a permis la mise en œuvre de « traitements automatisés de données à caractère personnel dénommés : *« bases d'analyse sérielle de police judiciaire », ayant pour finalité de rassembler les preuves et d'identifier les auteurs des crimes ou délits présentant un caractère sériel, grâce à l'établissement de liens entre les individus, les évènements ou les infractions »*[702]. Les données sont collectées lors d'enquêtes ou sur commission rogatoire lorsque la peine encourue est d'au moins cinq ans d'emprisonnement ou dans les enquêtes en matière de recherche des causes de la mort[703]. Ces traitements sont accessibles aux agents de

---

existe des indices graves et concordants laissant penser qu'elles aient pu participer à une infraction punie d'au moins 5 ans d'emprisonnement ; du nom, date de naissance, adresse et photographie des personnes dont on peut sérieusement penser qu'elles aient commis ou tenter de commettre une telle infraction, ou qu'elles sont en mesure de fournir des informations utiles relative à ladite infraction ; du nom, surnom, alias, sexe, date et lieu de naissance, adresse, photographie, éléments sur le mode de vie, s'agissant des personnes victimes d'une telle infraction ou faisant l'objet d'une enquête pour recherche des causes de la mort ou disparition.

[697] Par exemple, le SALVAC a permis en 2009 d'appréhender une personne suspectée d'avoir commis 11 viols entre 2003 et 2007 dans plusieurs villes. L'ADN du suspect avait été recueillie mais l'interrogation du FNAEG n'avait fait ressortir aucun profil enregistré mais avait permis de rattacher cette enquête à plusieurs autres. En 2009, le SALVAC a permis de faire le lien entre plusieurs enquêtes en comparant notamment le mode opératoire ainsi que certains éléments récurrents dans les différentes affaires (notamment l'odeur du suspect dont plusieurs victimes avaient fait état).
Voir à ce sujet, E. Pelletier, « Dix ans après, le violeur à la montre enfin arrêté », Le parisien, 15 décembre 2016. Et, J. Carpentier, « Neuf ans après les faits, le viol d'une joggeuse enfin élucidé », La voix du Nord, 16 décembre 2016.

[698] Article 230-13 du code de procédure pénale.

[699] Cour d'assises de Nancy le 28 avril 2016.

[700] Article L. 235-1 du code de la sécurité intérieure.

[701] Décret n° 2013-1054 du 22 novembre 2013 relatif aux traitements automatisés de données à caractère personnel dénommés « bases d'analyse sérielle de police judiciaire ».

[702] Article 1er, du décret 22 novembre 2013 relatif aux traitements automatisés de données à caractère personnel dénommés « bases d'analyse sérielle de police judiciaire ».

[703] *Ibid.*

gendarmerie ou de police individuellement désignés et spécialement habilités[704], aux magistrats du Parquet, aux juges d'instruction et aux agents des douanes individuellement désignés et spécialement habilités. Les données visées par ces traitements sont précisées en annexe du décret. Comme pour le SALVAC, ces données peuvent concerner les mis en cause, victimes et personnes susceptibles d'apporter des informations utiles. Il s'agit de collecter des données relatives à l'identité précise, l'adresse, la situation familiale, la profession, le comportement et tout élément relatif à l'infraction. Ces données sont conservées quinze ans pour les délits et vingt ans pour les crimes. La CNIL a eu à se prononcer préalablement à l'adoption du décret dans sa délibération du 20 septembre 2012[705]. Elle soulève que les traitements dont il est question ont pour finalité de rassembler des preuves et identifier les auteurs d'infractions ayant un caractère sériel et que ces finalités sont conformes aux dispositions du code de procédure pénale[706]. La commission fait référence à une « *même finalité générale, à savoir identifier les auteurs de crimes et délits punis de plus de cinq ans d'emprisonnement et présentant un caractère sériel»*[707]. La commission ajoute que ces traitements peuvent néanmoins *« différer sur la nature des infractions concernées »* sans que cela ne contrevienne aux dispositions de la loi informatique et libertés du 6 janvier 1978[708]. La commission précise que ces traitements ne peuvent pas servir aux fins d'enquêtes administratives et qu'ils sont alimentés uniquement par des procédures judiciaires. Concernant la collecte de données relatives au « comportement », la commission estime que ces données ne touchent pas aux données sensibles au sens de l'article 6 de la loi informatique et libertés. La CNIL a toutefois émis quelques réserves. C'est le cas par exemple du traitement des données dites de connexion[709] qu'elle a jugé inopportun et non pertinent. La question de la collecte des données sensibles dans le cadre des traitements d'analyse sérielle a aussi était abordée par la commission. Rappelant l'article 230-12 du code de procédure pénale, le décret prévoit le traitement de données sensibles dans la *« stricte mesure nécessaire aux finalités*

[704] Dans les conditions de l'article R. 40-35 du code de procédure pénale.
[705] Délibération n° 2012-321 du 20 septembre 2012 portant avis sur projet de décret relatif à la mise en œuvre de fichiers d'analyse sérielle dénommés « bases d'analyse sérielle de police judiciaire » (demande d'avis n° 12012464).
[706] Plus précisément l'article 230-12 prévoyant la possibilité pour les services d'enquête de mettre en œuvre des traitements afin de rassembler des preuves relatives aux infractions et d'établir des liens entre ces infractions ayant un caractère sériel.
[707] Délibération n° 2012-321 du 20 septembre 2012 portant avis sur projet de décret relatif à la mise en œuvre de fichiers d'analyse sérielle dénommés « bases d'analyse sérielle de police judiciaire » (demande d'avis n° 12012464).
[708] Notamment l'article 31 IV qui dispose que « les traitements qui répondent à une même finalité, portent sur des catégories de données identiques et ont les mêmes destinataires ou catégories de destinataires peuvent être autorisés par un acte règlementaire unique ».
[709] Il s'agit des mots de passe et des informations permettent leur vérification ou modification.

d'analyse sérielle assignées auxdits traitements »[710]. Concernant la collecte du groupe sanguin, la commission a toutefois demandé au ministère de préciser en annexe que cette dernière n'est possible que dans le cadre de recherche des causes de la mort ou de disparition. Là encore, la CNIL porte une attention particulière au respect du principe de finalité des données collectées.

Se pose aussi la question du rapprochement judiciaire à proprement parler, renvoyant aux logiciels permettent la mise en corrélation de données.

B. Les logiciels de rapprochement judiciaire

245. Logiciels de rapprochement – Les logiciels de rapprochement judiciaire permettent de *« faciliter l'exploitation et le rapprochement d'informations »*[711] recueillies au cours d'enquêtes. Comme en matière d'analyse sérielle, le décret du 7 mai 2012[712] a précisé les dispositions relatives au recours aux logiciels de rapprochement judiciaire et prévoit que la mise en œuvre de rapprochements judiciaires doit être autorisée par le magistrat en charge de l'enquête ou de l'instruction[713]. L'utilisation et le recours aux logiciels de rapprochement judicaire est encadré par la loi n° 2011-267 du 14 mars 2011[714]. Plus précisément, l'article 14 de la loi codifie aux articles 230-20 et suivants du code de procédure pénale des dispositions relatives aux logiciels de rapprochement judiciaire[715].

Néanmoins, le recours aux méthodes d'analyse criminelle préexistait à la loi de 2011 et des logiciels étaient utilisés bien avant son entrée en vigueur[716]. C'est notamment le cas

---

[710] Article 1er, Décret n° 2013-1054 du 22 novembre 2013 relatif aux traitements automatisés de données à caractère personnel dénommés « bases d'analyse sérielle de police judiciaire.

[711] Article 230-20 du code de procédure pénale.

[712] Décret n° 2012-689 et n° 2012-687 du 7 mai 2012 relatif à la mise en œuvre de logiciels de rapprochement judiciaire à des fins d'analyse criminelle.

[713] Article R. 40-40 du code de procédure pénale.

[714] Loi n° 2011-267 du 14 mars 2011 dite LOPPSI 2, modifiée par la loi n° 2013-1117 du 6 décembre 2013 relative à la lutte contre la fraude fiscale et la grande délinquance économique et codifiée aux articles 230-20 et suivants du code de procédure pénale s'agissant des logiciels de rapprochement judiciaire.

[715] V. Gautron, « Fichiers de police », Répertoire de droit pénal et procédure pénale, *op. cit*.

[716] Le recours à la méthode d'analyse criminelle est souvent rattaché à l'affaire Joseph Vacher relative à des crimes en série perpétrés dans les années 1890 et condamné à mort le 13 décembre 1898 pour les faits de meurtres et viols. Dans cette affaire plusieurs juges d'instructions vont se succéder et l'un d'entre eux va initier ce qu'on appelle aujourd'hui le profilage criminel. En opérant des comparaisons entre les différentes pièces de l'enquête, il finit par faire le lien entre différents crimes perpétrés à différents endroits à une époque où il n'y a pas encore de police nationale et où les enquêtes sont donc limitées aux frontières des départements. La méthode d'analyse criminelle va permettre à l'époque d'identifier l'auteur des crimes (bien qu'il ne fut jugé et condamné que pour un seul). Cette affaire reste importante à plusieurs égards. Tout d'abord, puisqu'il s'agit d'une des premières enquêtes de crimes en série. Ensuite, l'enquête initie les bases de l'analyse criminelle et des méthodes de profilage. Enfin, il faut noter que plusieurs expertises médico-légales avaient été ordonnées soulevant déjà à l'époque la question de la responsabilité pénale des aliénés.

d'ANACRIM (pour ANAlyse CRIMinelle). Créé par la loi n° 2003-239 du 18 mars 2003[717] le logiciel ANACRIM est présenté comme un outil de travail ayant pour finalité de faciliter les enquêtes en créant des liens entre différentes données et en rendant de ce fait plus lisibles les différentes informations, notamment en matière d'enquêtes *« complexes »*[718] ou présentant un caractère sériel. Ce logiciel utilise les données de fichiers dits *« temporaires »* de données collectées pendant les enquêtes. Il opère une analyse[719] des données permettant *« d'orienter »* les investigations. Les fichiers temporaires peuvent contenir toutes les informations recueillies lors d'enquêtes sans qu'une liste exhaustive ne soit fixée. Les analyses effectuées sont alors accessibles aux services de police judiciaire, aux magistrats chargés de l'enquête ainsi qu'aux avocats des différentes parties[720]. Les données collectées dans les fichiers de travail temporaires ne sont conservées que le temps de l'analyse et sont systématiquement détruites après. Seules les conclusions de ces analyses sont conservées[721].

246. L'encadrement par la loi du 14 mars 2011 – La loi du 14 mars 2011 est venue officialiser et encadrer le recours à cette pratique. Ainsi, les logiciels de rapprochement visent à *« faciliter le rassemblement des preuves des infractions et l'identification de leurs auteurs »*[722] pour les services d'enquêtes et d'instruction. Les données à caractère personnel contenues dans ces logiciels sont conservées trois ans ou le temps nécessaire à l'enquête[723]. Ces logiciels sont placés sous le contrôle du procureur de la République qui dispose d'un accès direct à ces derniers. Les données sont accessibles aux services de police judiciaire individuellement désignés et spécialement habilités ainsi qu'aux magistrats du Parquet et aux magistrats instructeurs. Il s'agit donc pour ces services de recouper des données collectées

---

Voir à ce sujet, M. Renneville, L'affaire Joseph Vacher : la fin d'un brevet d'impunité » pour les criminels ?, *Droit et cultures*, février 2010, p. 129-142.

[717] Loi n° 2003-239 du 18 mars 2003 pour la sécurité intérieure, modifiée par la loi n°2005-1549 du 12 décembre 2005 relative au traitement de la récidive des infractions pénales.

[718] Rapport du groupe de contrôle des fichiers de police et gendarmerie. Les auteurs définissent ici la notion de complexité de l'enquête eu égard à la multitude de pièces de procédure ainsi qu'à leur nature variées.

[719] Cette analyse constitue une analyse du cas précis de l'enquête en cours, une analyse comparative, une analyse quant à la personnalité de l'auteur ainsi qu'une analyse du groupe le cas échéant.

[720] En application des dispositions de l'article 114 du code de procédure pénale concernant l'accès au dossier d'instruction par les avocats des mis en cause et parties civiles.

[721] Rapport du groupe de contrôle des fichiers de police et gendarmerie, *op. cit.* .Les auteurs opèrent le distinguo entre fichiers judiciaires d'antécédents et fichiers temporaires d'investigations judiciaires.

[722] Article 230-20 du code de procédure pénale.

[723] Il convient de noter que les dispositions initiales relatives à la durée de conservation des données ont été déclarées non conformes à la Constitution dans une décision n° 2011-265 DC du 10 mars 2011. Ces dernières prévoyaient une conservation de trois ans à compter du dernier acte d'enregistrement et ce peu importe la gravité des faits.

lors d'enquêtes et d'opérer un rapprochement pertinent entre ces informations[724]. La CNIL a eu à se prononcer sur les projets de décrets relatifs à la mise en œuvre des logiciels de rapprochement judiciaire. Sur le régime juridique ainsi que sur la finalité des logiciels et la nature et durée de conservation des données la commission n'a pas émis d'observations particulières. Toutefois, cette dernière a soulevée la question des missions confiées au procureur de la République et au magistrat référent en charge du contrôle de ces logiciels. La commission considère que ces missions ne sont pas suffisamment détaillées. Elle soulève également l'importance d'une traçabilité des actions opérées sur ces logiciels[725].

Les logiciels d'analyse criminelle permettent donc une nouvelle lecture des procédures mettant en avant des concordances et incohérences dans des dossiers comportant parfois des milliers de pièces. Ces logiciels ont permis des avancées considérables dans des instructions parfois fastidieuses. Le logiciel a notamment été utilisé dans l'instruction de l'affaire dite de Grégory Villemin par le service central de renseignements criminels (SCRC)[726]. S'il est fait souvent référence au SALVAC ou à ANACRIM, il existe d'autres logiciels utilisés dans le même but[727].

Au-delà du simple rapprochement, les données font l'objet de véritables interconnexions c'est-à-dire que les fichiers peuvent automatiquement être mis en relation les uns avec les autres et s'alimenter entre eux.

§2. L'interconnexion entre fichiers judiciaires nationaux

247. Interconnexion de fichiers – L'interconnexion est un processus automatisé visant à mettre en corrélation des données issues de fichiers auparavant distincts. La notion d'interconnexion n'a pas été définie strictement par la loi informatique et libertés mais la CNIL a dégagé des critères cumulatifs permettant de mieux encadrer la notion en se fondant

[724] L'article 230-21 du code de procédure pénale précise bien que ces données « ne peuvent provenir que de pièces et documents de procédure judiciaire déjà détenus par les services ».

[725] Délibération CNIL n° 2011-418 du 15 décembre 2011 portant avis sur un projet de décret relatif à la mise en œuvre de logiciels de rapprochement judiciaire à des fins d'analyse criminelle (demande d'avis n° 1523917). A noter que sur la question de la traçabilité des opérations effectuées sur les logiciels, l'article 4 du décret 2012-687 du 7 mai 2012 prévoit que soit conservée une trace des consultations et plus précisément l'identité de la personne ayant eu accès aux données et ce pour une période de 5 ans.

[726] Dans le cadre de l'instruction ouverte suite au meurtre de Grégory Villemin en 1984, le logiciel ANACRIM a récemment été interrogé et ceci a permis d'envisager de nouvelles pistes dans l'instruction du dossier.

[727] On peut citer par exemple le logiciel d'analyse criminelle d'uniformisation des procédures d'identification (LUPIN) créé par arrêté du 15 octobre 2014 (JO 24 octobre), la cellule opérationnelle de rapprochement et d'analyse des infractions liées (CORAIL) et le partage de l'information opérationnelle (PIO) créés par le décret n° 2014-187 du 20 février 2014 qui permettent le traitement et la diffusion de l'information au sein des services d'enquête.

sur des notions qui ont été mis en exergue par le Conseil d'Etat[728]. Ainsi, l'interconnexion vise à mettre en relation des traitements de données à caractère personnel. Cette opération doit viser au moins deux fichiers distincts et répondre à un processus automatisé (ce qui la distingue du simple rapprochement de données). Enfin, l'interconnexion met en relation des fichiers ayant initialement des finalités distinctes. Ce dernier point soulève d'ailleurs le plus d'interrogations puisqu'il met à mal le principe protecteur de finalité dégagé par la CNIL. Il ne fait aucun doute que l'interconnexion est la conséquence du développement de la bureautique et d'internet qui ont facilité le partage et la communication des données.

Par principe, toute interconnexion de fichiers doit faire l'objet d'une autorisation préalable de la CNIL.

Ce mécanisme d'interconnexion peut donc permettre une mise en relation de fichiers réciproque ou à sens unique et être mise en œuvre de manière permanente ou ponctuelle mais toujours de manière automatisée.

Les interrogations liées à l'interconnexion des fichiers de données judiciaires ne sont pas nouvelles. Il faut se rappeler l'affaire dite du projet « Safari » en 1974 qui visait justement à centraliser les données de la police judiciaire et des services de renseignements. Néanmoins à la suite de vives oppositions dont il avait fait l'objet, ce projet a été abandonné et a même conduit à l'adoption de la loi informatique et libertés de 1978. Ainsi, l'article 33 de la loi pose le principe selon lequel toute interconnexion de fichiers relevant d'entités différentes et ayant une finalité différente doit être soumise à avis préalable de la CNIL, interconnexions qui relevaient néanmoins du régime d'autorisation supprimé lors de l'adoption du « paquet européen » sur la protection des données.

Là où certains parlent d'un retour à l'Etat protecteur ou du développement d'un Etat sécuritaire, d'autres y voient la condition nécessaire à la protection des individus[729].

L'interconnexion des fichiers de police soulève de nombreuses interrogations. Certains y voient le moyen de garantir l'efficacité des outils de prévention et de lutte contre les infractions (A.), d'autres évoquent des risques pour les libertés face à une société de plus en plus sécuritaire (B.).

[728] CE 19 juillet 2009, 10e et 9e sous sections réunies, n° 317182, « L'interconnexion doit être regardée comme l'objet même d'un traitement qui permet d'accéder à, d'exploiter et de traiter automatiquement les données collectées pour un autre traitement et enregistrées dans le fichier qui en est issu ».

[729] A ce sujet voir, J.J. Lavenue, « Interconnexion des fichiers : de la réduction du champ des libertés au retour de l'Etat protecteur », *in Terminal*, 112/2013, p. 125-140.

J.J. Lavenue, L'interopérabilité et l'interconnexion des fichiers de police : enjeux et ambigüité du rapport dialectique entre principe d'efficacité et protection des libertés, *op. cit.*, 2014.

A. L'interconnexion outil d'efficacité et de fiabilité

248. Outil d'efficacité – Il ne fait nul doute que le développement de nouveaux moyens de communication a permis de créer des outils plus efficaces en matière de procédures judiciaires. Il faut aussi noter que le développement de nouvelles formes de criminalité (criminalité organisée de manière générale) rend nécessaire l'utilisation de tels outils. Ce constat d'un besoin en termes d'efficacité conduit à conclure à la nécessité et à l'utilité de ces moyens. Il ne s'agit pas ici de dresser une liste exhaustive des interconnexions existantes en matière judiciaire mais de présenter les principales ainsi que leur fonctionnement et utilité.

249. Interconnexion entre le TAJ et Cassiopée – Toujours dans l'optique du partage des données de la chaine pénale, le nouveau système d'information lié à l'investigation (NS2i) a permis l'interconnexion du TAJ et de Cassiopée. L'interconnexion des deux fichiers doit permettre une meilleure mise à jour et un suivi des procédures en temps réel, Cassiopée ayant lui-même permis une mise en commun des données des bureaux d'ordre au niveau national. L'interconnexion permet de « fiabiliser » les données des fichiers[730]. Cette interconnexion avait déjà fait l'objet d'une proposition dans le rapport d'information déposé à l'assemblée nationale par la commission des lois en 2009[731].

250. Interconnexion entre les logiciels de rédaction et Cassiopée – Dans une moindre mesure on peut citer l'interconnexion entre les logiciels de rédaction de procédures utilisés en gendarmeries et commissariats de police avec le logiciel Cassiopée utilisé par les Parquets. Il ne s'agit pas de « fichiers » à proprement parler mais bien de traitements de données puisqu'il s'agit de logiciels permettant la saisie de données et ayant vocation à alimenter automatiquement des fichiers. En cela, il peut être intéressant de s'intéresser à cette interconnexion avec « CASSIOPEE ». Ces logiciels d'aide rédactionnelle nommés LRPPN (pour Logiciel de rédaction des procédures de la police nationale) et sa version LRPGN utilisée en gendarmeries ont été créés en remplacement du logiciel ARDOISE (Application de

[730] Institut National des hautes études de la sécurité et de la justice, « Fichiers de police et libertés : des enjeux nationaux, une nouvelle donne internationale », Travaux des auditeurs, Rapport du Groupe de diagnostic stratégique n°6 – 25e Session nationale « Sécurité et Justice » - 2013/2014.

[731] Rapport d'information de la commission des lois constitutionnelles, de la législation et de l'administration générale de la République sur les fichiers de police, Députés Batho D. et BENISTI J-A, déposé le 24 mars 2009. Dans ce rapport, les députés dans le point n°34 proposaient de *« mettre en place au plus vite le dispositif d'échanges d'informations entre CASSIOPEE et ARIANE, afin de tenir compte plus rapidement et plus efficacement des changements de qualification et des suites judiciaires »*. (ARIANE étant un fichier d'antécédents antérieur à l'entrée en vigueur du TAJ).

recueil de la documentation opérationnelle et d'informations statistiques sur les enquêtes)[732]. Initialement, ces logiciels permettaient de rédiger les procédures mais n'alimentaient aucun autre traitement. Le logiciel LRPPN 2 a été créé après avis de la CNIL du 11 octobre 2012[733] par le décret du 17 décembre 2013[734]. Le but de cette nouvelle version était notamment d'informatiser et d'automatiser la chaine pénale du premier enregistrement à la fin de la procédure. Le décret a créé une interconnexion entre les logiciels de rédaction de procédures (LRPPN et LRPGN) et Cassiopée. Ainsi, les services des bureaux d'ordre des Parquets peuvent être en mesure de récupérer les données saisies lors de la rédaction des procès-verbaux. Le décret prévoit également la possibilité d'alimenter d'autres fichiers notamment le traitement des antécédents judiciaires (TAJ) ou le fichier des objets et véhicules signalés (FOVES). La CNIL a considéré que l'interconnexion entre LRPPN 2 et le TAJ permettrait une mise à jour automatique des données et pourrait de ce fait répondre à la problématique qui avait été soulevée au préalable des erreurs contenues dans le fichier suite à la récupération des données du STIC. Pour rappel, le TAJ a été créé par la fusion entre le STIC et le JUDEX et la commission avait déploré que cette fusion se fasse sans avoir, au préalable, purgé les deux fichiers des erreurs qu'ils contenaient[735]. Cette interconnexion permettrait selon elle d'effectuer une mise à jour des données du TAJ. La commission émet toutefois une réserve relative à la confidentialité des données qui seront transmises.

Face à ce constat de l'utilité avérée de ces dispositifs, il convient néanmoins de s'interroger sur la place des libertés individuelles dans le développement de tels outils.

B. L'interconnexion et les risques pour des libertés individuelles

251. Interrogations liées à l'interconnexion – L'interconnexion des fichiers de police soulève différentes interrogations et craintes. Bien que favorable à cette interconnexion dans l'hypothèse où elle favorise la mise à jour des données, la CNIL a émis quelques réserves face

[732] ARDOISE a remplacé le logiciel de rédaction des procédures (LRP), lui-même remplacé par le logiciel de rédaction des procédures de la police nationale (LRPPN) mis en œuvre par le décret n° 2011-110 du 27 **janvier 2011** autorisant la création d'un traitement automatisé de données à caractère personnel dénommé Logiciel de rédaction des procédures de la police nationale (LRPPN).

[733] Décision CNIL 2012-365 du 11 octobre 2012 portant avis sur un projet de décret relatif modifiant le décret n° 2011-110 du 27 janvier 2011 portant création d'un traitement automatisé de données à caractère personnel dénommé LRPPN 2. Demande d'avis n° 12017917.

[734] Décret n°2013-1169 du 17 décembre 2013 portant création d'un traitement automatisé de données à caractère personnel dénommé LRPPN 2.

[735] Voir à ce sujet les conclusions du groupe de contrôle des fichiers d'antécédents du ministère de l'intérieur adopté par la CNIL en assemblée plénière le 13 juin 2013.

à l'accroissement de ce phénomène[736]. La commission fait référence à quatre « risques majeurs » liés à l'interconnexion de fichiers. Le premier et le plus évident est celui lié à l'interconnexion de fichiers ayant à l'origine des finalités distinctes et qui de ce fait tend à modifier la finalité initialement déterminée. La Commission parle même *« d'extension occulte du champ du fichier »*[737]. Ensuite, la CNIL s'interroge sur les risques en termes de secrets professionnels. Les données soumises au secret pourraient se voir soumises à un régime moins protecteur lorsqu'elles sont récupérées par un autre fichier. De la même manière, la durée de conservation fixée dans le fichier destinataire pourrait être plus longue que celle du fichier d'origine. Enfin de manière plus générale, la commission s'est interrogée sur la question de la sécurité des données lors de ces interconnexions et du transfert des données.

252. Garanties existantes – Il existe toutefois certaines garanties législatives. Par exemple, aucune interconnexion n'est possible entre le casier judiciaire national et tout autre fichier de données à caractère personnel. Les données de ce dernier ne sont accessibles que sur demande expresse[738]. Aussi, le FNAEG ne peut, en principe, faire l'objet d'aucune interconnexion. De manière générale, les interconnexions visent les fichiers d'antécédents et si elles permettent une mise à jour en temps réel il parait évident qu'elles permettent de la même manière la récupération de données erronées ce qui en fait parfois une source d'erreurs. S'agissant du FNAEG, le décret du 18 mai 2000[739] est venu préciser les modalités de mise en œuvre du fichier. Il modifie les dispositions du code de procédure pénale et notamment l'article R53-19 qui précise que toute interconnexion entre le fichier et tout autre fichier est prohibée. Ces dispositions s'appliquent également au rapprochement de données sous réserve des dispositions de l'article R53-20 qui prévoit que ces données pourront faire l'objet d'un enregistrement sous un numéro d'ordre commun avec le fichier du service central.
Le partage de données fichées trouve aussi à se poser au niveau international soulevant d'autant plus d'interrogations.

[736] Rapport d'information n°4113 enregistré le 21 décembre 2011, *op. cit.*, p.96 et suivantes.
[737] *Ibid.*
[738] Art. R.76 et suivants du code de procédure pénale.
[739] Décret n°2000-413 du 18 mai 2000 modifiant le code de procédure pénale et relatif au fichier national automatisé des empreintes génétiques et au service central de préservation des prélèvements biologiques.

Section 2 : Le partage de données à caractère personnel au niveau international dans le cadre de la coopération policière et judiciaire

253. Un partage nécessaire – Dans le cadre judiciaire[740], les données sont nécessairement amenées à être échangées entre Etats. Lors d'enquêtes, les Etats sont amenés à déposer des demandes afin d'obtenir certaines données mais il peut également s'agir de données mises à dispositions de ces derniers dans un cadre très précis. Quoi qu'il en soit, cet échange de données est très strictement encadré car il soulève bien évidemment des questions en termes de sécurité des données à caractère personnel. Il va de soi que les questions d'ores et déjà soulevées dans le cadre du transfert de données *intra muros* trouvent évidemment d'autant plus à se poser en matière d'échanges internationaux.

L'idée d'une coopération judiciaire et policière n'est pas nouvelle et a émergé dès les premiers grands conflits mondiaux. Les conflits actuels auxquels doivent faire face les Etats et l'émergence de nouvelles formes de criminalité a sans nul doute favorisé le développement de ces coopérations obligeant les différents pays à mettre en commun certaines informations.

Il s'agit ici de s'interroger sur le transfert de données à caractère personnel dans le cadre de cette coopération judiciaire et policière telle qu'elle est mise en œuvre de nos jours et sur ces éventuelles évolutions.

254. La consécration des affaires intérieures – L'ouverture des frontières par les accords de Schengen[741] ont conduit à l'établissement de mesures dites compensatoires instaurant un système commun de contrôle aux frontières. Par la suite, le traité de Maastricht[742] consacre les affaires intérieures au sein de son troisième pilier. Il s'agit de créer un cadre structurel en matière de coopération judiciaire et policière garantissant les intérêts communs de tous les Etats membres. La coopération est alors soumise à la méthode dite « intergouvernementale » c'est à dire que les décisions sont prises à l'unanimité par les membres du Conseil de l'Europe sur proposition soit de la Commission européenne soit des Etats membres. Le traité instaure également de nouveaux domaines en matière de coopération en créant notamment la politique

[740] Voir *infra* n°

[741] Accords de Schengen du 14 juin 1985 signés initialement par la France, l'Allemagne, la Belgique, le Luxembourg et rejoint petit à petit par les autres pays membres. A noté néanmoins que la convention d'application ne sera signée qu'en 1990 et entrera en vigueur en 1995.

[742] Le traité de Maastricht a été signé le 7 février 1992 par les 12 pays membres. Les 17 et 28 février 1986, l'Acte unique européen était signé par douze Etats et avait pour but de relancer la construction de l'Europe.
Le traité de Maastricht apparaît comme marquant un tournant dans cette construction en prévoyant notamment la création d'une monnaie unique, en créant une véritable citoyenneté européenne et également en créant le troisième pilier consacré à la justice et aux affaires intérieures (JAI).

étrangère et de sécurité commune (PESC) consacrée au sein du deuxième pilier. Plus spécifiquement, le troisième pilier prévoit les dispositions relatives à la coopération policière et judiciaire dans l'Union européenne[743]. Le Traité d'Amsterdam signé le 2 octobre 1997 prévoit le renforcement de la coopération internationale instaurant les bases de la coopération judiciaire et policière en matière pénale. Suite à l'abandon du troisième pilier par le traité de Lisbonne du 13 décembre 2007, la coopération judiciaire repose désormais sur un fonctionnement communautaire c'est-à-dire que les décisions sont prises à la majorité qualifiée[744]. Cette coopération repose à la fois sur des traités, des conventions, des décisions-cadre, ainsi que un grand nombre d'acteurs intervenant sur des domaines de compétence spécifiques et complémentaires. Aussi, cette coopération s'étend bien au delà des frontières de l'Union européenne[745].

Il s'agit donc de s'intéresser au cadre structurel et institutionnel de la coopération judiciaire et policière (I.), puis aux acteurs de la coopération judiciaire et policière (II.).

§1. Le cadre structurel et institutionnel de la coopération judiciaire et policière

255. Cadre structurel – La coopération judiciaire et policière actuelle est le fruit des différentes évolutions antérieures et s'appuie sur les différents acquis de ces anciens systèmes, comme notamment l'acquis Schengen. Ces différentes formes de coopération ont dû s'adapter aux évolutions de la société moderne dont ils ont su tirer parti et aux évolutions de la criminalité. Les échanges de données à caractère personnel dans le cadre de cette coopération ont nécessairement évolué avec le développement des moyens de communication et également avec le développement des nouvelles formes de données judiciaires.

Il convient donc de s'intéresser au partage de données à caractère personnel dans le cadre de l'acquis Schengen (A.), des régimes dérogatoires applicables avec les Etats n'adhérant pas à Schengen (B.), de la coopération renforcée (C.)

[743] La coopération internationale n'est pas nouvelle et s'est dans un premier temps développée de manière moins formelle en matière policière au travers du « groupe de Trévi » en 1976. Il s'agit à l'époque d'un réseau intergouvernemental composé de représentants des ministères et des affaires étrangères. Le traité de Maastricht est venu par la suite préciser les champs d'intervention de cette coopération et l'officialiser. Le groupe sera remplacé par l'actuel Europol avec la signature de la convention du 26 juillet 1995.

[744] S'agissant des décisions en matière de coopération policière, le rapprochement des législations pénales ou la création d'un Parquet européen, celles-ci se font toujours à l'unanimité.

[745] Sur l'historique de la coopération internationale et la présentation des différents acteurs ainsi que du cadre structurel, voir, H. Labayle, C*oopération judiciaire et policière en matière pénale*, Jurisclasseur Europe, 3 décembre 2017.

A. Le partage de données à caractère personnel dans le cadre de l'acquis Schengen

256. Acquis Schengen – L'acquis Schengen renvoie tant à l'accord signé initialement en 1985, qu'à la convention d'application ainsi qu'aux accords d'adhésion ratifiés par la suite par différents Etats membres ou aux décisions prises par la Comité exécutif. Suite à l'intégration de l'acquis Schengen dans le droit de l'Union européenne, d'autres décisions et accords ont été pris sur le même modèle. Les accords de Schengen et plus encore leur convention d'application marque la « relance de la coopération policière et judiciaire en Europe »[746]. Si la coopération internationale a débuté bien avant les accords de Schengen, ces derniers marquent néanmoins *« le premier succès institutionnalisé de l'approche intergouvernementale de la coopération policière »*[747]. En ouvrant les frontières et en supprimant le contrôle aux frontières internes, les accords de Schengen vont mettre en place toute une série de mesures nécessitant pour les Etats membres une plus grande communication et un partage de données.
Dans le cadre des mesures compensatoires à l'ouverture des frontières, les Etats membres sont amenés à partager des données qu'ils détiennent. Il convient de s'intéresser au cadre de mise en œuvre de la surveillance aux frontières (1°) afin de s'interroger sur le partage de données dans le cadre du renforcement de la coopération policière et judiciaire (2°)

1° Le cadre de mise en œuvre de la surveillance des frontières extérieures

257. Assistance commune – L'ouverture des frontières a nécessité la mise en œuvre de mesures visant à compenser les conséquences de la suppression des contrôles aux frontières internes à l'espace Schengen. Les Etats parties à la convention coopèrent dès lors afin d'assurer ensemble la surveillance des frontières extérieures nécessitant de ce fait le partage de données. Dans le cadre de cette coopération a été instaurée une véritable politique commune matière de sécurité.
Ainsi, les articles 39 à 59 de la convention d'application de l'accord Schengen prévoient les dispositions relatives à la coopération policière et judiciaire. Aux termes de ces dispositions, les Etats *« s'engagent à ce que leurs services de police s'accordent, dans le respect de la législation nationale et dans la limite de leurs compétences, l'assistance aux fins de la*

[746] V. Gaudin, E. Roux, *Coopération policière internationale*, Répertoire de droit pénal et de procédure pénale, octobre 2010, actualisation octobre 2017.
[747] *Ibid.*

prévention et de la recherche de faits punissables »[748]. Les données visées par ces dispositions ne peuvent être utilisées qu'aux fins de preuve[749] et sont échangées entre les autorités compétentes des Etats chargés de la coopération internationale[750]. Ces missions relèvent pour la France des officiers et agents de police judiciaire et de gendarmerie sous le contrôle de la direction centrale de la police judiciaire. Ces dispositions ne s'opposent pas à ce que des accords bilatéraux soient conclus entre les Etats. Cette coopération peut revêtir différentes formes.

258. Obligation d'assistance mutuelle – L'obligation d'assistance mutuelle prévue à l'article 39 de la convention d'application suppose que les Etats signataires apportent respectivement leur soutien à la recherche et à la prévention des infractions. Pour ce faire, ces derniers doivent échanger des informations entre services de police et de gendarmerie. Ces informations renvoient à toutes données à caractère personnel telles que plaques minéralogiques de véhicules, numéros de téléphone, adresses et peuvent également faire référence aux antécédents judiciaires. Ces données peuvent être collectées afin de servir de preuve d'une infraction et avec l'accord de l'Etat duquel elles proviennent. Une circulaire du 23 juin 1995[751] est venue préciser les modalités de partage de ces données indiquant tout d'abord qu'il s'agit dans la pratique de copies de procès-verbaux et de procédures judiciaires. La circulaire opère une distinction entre les données transmises de la France à l'étranger et celles transmises de l'étranger à la France. Assez logiquement, les données qui seront demandées à la France alors qu'une information judiciaire est ouverte le seront sur autorisation du juge d'instruction. Dans les autres cas, la délivrance de cette autorisation relève du procureur de la République[752]. Il pourra alors s'agir pour la France de transmettre au pays demandeur des copies d'auditions, des expertises, des interrogatoires ou tout document obtenu dans le cadre de commission rogatoire. Pour les demandes adressées à la France, la circulaire précise qu'il appartient au magistrat chargé de délivrer l'autorisation de vérifier que ce partage de données ne risque pas de mettre en péril la procédure française. Sur la forme, cette autorisation ne doit observer aucun formalisme particulier mais la demande doit être transmise au pays requérant par l'intermédiaire du ministère de la justice. Ensuite, les

[748] Art. 39§1 de la convention d'application de l'accord Schengen.
[749] Art. 39§2 de la convention d'application de l'accord Schengen.
[750] Art. 39§ de la convention d'application de l'accord Schengen.
[751] Circulaire du 23 juin 1995 commentant les dispositions des articles 39, 40 et 41 de la convention signée à Schengen le 19 juin 1990. JORF n° 152 du 1er juillet 1995.
[752] Conformément à l'article R. 156 du code de procédure pénale.

données sont transmises par le biais de la Direction centrale de la police judiciaire[753]. Concernant les demandes adressées par la France à un autre pays signataire, ces dernières doivent également être transmises par le ministère de la justice[754]. On constate donc que dans le cadre de la coopération internationale et de l'obligation d'assistance mutuelle des données issues de procédures judiciaires parfois en cours peuvent faire l'objet d'un partage avec des pays tiers.

259. Observation transfrontalière – L'article 40 de la convention d'application de l'accord Schengen consacre le droit d'observation. Ce droit permet à un pays signataire qui aurait constaté sur son territoire la présence d'un individu soupçonné d'avoir commis un fait punissable de continuer la surveillance de ce dernier sur le territoire d'un autre pays signataire. L'infraction doit être susceptible de donner lieu à extradition[755]. Cette démarche nécessite d'obtenir l'accord du pays pour l'observation transfrontalière et prend la forme d'une demande d'entraide judiciaire. La convention et la circulaire du 23 juin 1995 opèrent une distinction tenant compte de l'urgence de la situation. Ainsi, en l'absence d'urgence et sur le même principe qu'en matière d'assistance, le droit d'observation transfrontalière doit être autorisé par l'Etat sur lequel il s'exerce. La demande prend la forme d'une demande d'entraide judiciaire communiquée à l'autorité désignée compétente[756] et délivrée par le ministère de la justice. L'observation peut également être confiée aux autorités judiciaires du pays sur lequel elle a lieu. En cas d'urgence, l'observation peut avoir lieu sans autorisation préalable mais est dans ce cas limitée à certaines infractions d'une particulière gravité[757]. Dans ce cas, l'autorité compétente doit être immédiatement informée dès le franchissement de la frontière et la demande d'entraide judiciaire doit intervenir dans les meilleurs délais. Si l'autorisation n'est pas délivrée dans les cinq heures, l'observation devra immédiatement cesser. De manière générale, les agents autorisés à exercer ce droit d'observation sont les officiers de police judiciaires et de gendarmerie. Une fois autorisé à agir, ces agents ne peuvent néanmoins effectuer que les actes qui pourraient être réalisés lors d'enquêtes locales

[753] En cas d'urgence, la demande peut être directement envoyée au magistrat compétent et les données transmises au requérant. Dans ce cas, le ministère en est informé par la suite.
[754] En cas d'urgence, l'autorisation et les données peuvent être transmises avant à la condition que l'autorisation soit fournie dans les plus bref délais.
[755] Conformément à l'article 61 de la convention Schengen soit une peine d'au moins deux ans d'emprisonnement selon la loi française. Article 696-3 du code de procédure pénale.
[756] L'article 40§5 de la convention d'application fixe les autorités compétentes pour délivrer cette autorisation. Il s'agit pour la France de la Direction centrale de police judiciaire.
[757] Sont concernées les infractions d'assassinat, meurtre, viol, incendie volontaire, fausse monnaie, vol et recel aggravés, extorsion, enlèvement et prise d'otage, trafic d'êtres humains, trafic illicite de stupéfiants…telles que définies à l'article 40§7 de la convention d'application.

par l'Etat sur le territoire duquel le droit est exercé. Il s'agit ici de respecter la législation interne de l'Etat. Ainsi, l'exercice de ce droit d'observation permet de procéder à des filatures, effectuer des constatations, prendre des photographies, recueillir des témoignages spontanés ou saisir des pièces qui seraient remises volontairement. Toutefois, les agents ne peuvent pas intercepter des correspondances émises par voie de télécommunication. L'article 40§3 interdit expressément de réaliser des perquisitions au domicile ou d'interpeller ou procéder à l'arrestation de la personne visée[758]. Là encore que ce soit par observation directe ou par le biais des agents locaux, ce mécanisme permet aux autorités étrangères d'accéder à des données personnelles relatives à des individus présents sur le territoire et aux autorités françaises d'accéder aux données relatives à des individus se situant dans un pays tiers. Toutefois, une fois l'observation terminée, un rapport doit être dressé et communiqué au ministère de la justice opérant ainsi un certain contrôle sur les données collectées. Le fait de ne pouvoir exercer que des actes qui seraient permis au niveau interne apporte également une certaine garantie.

A noter toutefois que le règlement 2017/458 du 15 mars 2017[759] entré en vigueur le 7 avril 2017 permet dans certains cas, liés notamment à la menace terroriste, de rétablir temporairement les contrôles internes modifiant ainsi le code frontières Schengen[760] et affaiblissant ainsi le principe de libre circulation et la règle de vérification minimale.

2° Le partage de données dans le cadre du renforcement de la coopération policière et judiciaire

260. Instauration du Système d'information Schengen (SIS) – Afin de compenser la suppression des frontières internes à l'espace Schengen, les coopérations policières et judiciaires ont été renforcées. Cette coopération repose essentiellement sur la création du Système d'information Schengen (SIS) outil informatique de signalements.

Le système d'information Schengen (SIS) est un fichier automatisé de traitement de données commun aux Etats membres de l'espace Schengen. Il centralise des données relatives notamment aux personnes recherchées ou surveillées par les autorités judiciaires, aux

[758] En vertu d'accords bilatéraux, Les agents des douanes français sont autorisés à exercer ce droit d'observation à l'étranger en matière de trafic de stupéfiants.

[759] Règlement (UE) 2017/458 du Parlement et du Conseil du 15 mars 2017 modifiant le règlement (UE) 2016/399 en ce qui concerne le renforcement des vérifications dans les bases de données pertinentes aux frontières extérieures.

[760] Le code frontières Schengen a été instauré par le règlement (CE) 562/2006 du Parlement européen et du Conseil établissant un code communautaire relatif au régime de franchissement des frontières par les personnes. Modifié par le règlement (UE) 610/2013 du Parlement européen et du Conseil du 26 juin 2013.

personnes disparues, aux personnes interdites de séjour sur le territoire d'un des Etats membres de l'espace Schengen ou encore aux véhicules et objets recherchés. En France, il est géré par la Direction générale de la police nationale et alimenté par le fichier des personnes recherchées[761] et par le fichier des véhicules volés. Plus précisément, le SIS contient des informations relatives à l'identité des personnes signalées (nom, prénom, alias, lieu de naissance, sexe, nationalité, signes physiques particuliers, photographies, empreintes digitales, motif du signalement, informations sur la dangerosité, type d'infractions et conduite à tenir ou mesures à prendre en cas d'interpellation de l'individu). Le fichier mentionne également tout lien avec d'autres signalements[762].

Les modalités encadrant ce fichier sont prévues aux articles 92 et suivants de la convention d'application. Plus précisément, le fichier comporte une partie nationale pour chaque Etat et une fonction support technique. L'idée est que tous les pays parties à la convention alimentent et accèdent aux données fichées notamment lors de contrôles aux frontières et de contrôles effectués à l'intérieur du territoire. Cette consultation s'effectue par une interrogation automatisée du fichier[763]. Le fichier a pour objet « la préservation de l'ordre et de la sécurité publics, y compris la sûreté de l'Etat»[764]. L'accès aux données est réservé aux agents compétents dans les différents pays en matière de contrôles aux frontières, douanes et services de police et gendarmerie ainsi qu'aux administrations chargées d'examiner les demandes de visas. Cet accès est régi par la législation interne de chaque pays[765]. Il est utile de mentionner que seules les données nécessaires peuvent être consultées. La liste des autorités autorisées à consulter le fichier doit être communiqué au Comité exécutif. Là encore, la liste exhaustive des données pouvant faire l'objet d'un fichage au SIS ainsi que les restrictions encadrant la consultation du fichier ont pour but d'assurer un certain contrôle sur les données et apporte une certaine garantie s'agissant de données partagées entre tous les Etats signataires de la convention.

261. Evolution vers le Système d'information Schengen II (SIS II) – Le fichier a été révisé en 2006 et est entré en vigueur en 2013 donnant naissance au fichier dit de deuxième génération le SIS II. La Commission européenne a été chargée dès 2001 de faire évoluer le fichier. Le Parlement européen considérant que le SIS I ne permettait plus de faire face au

[761] Voir *supra*. n°183.
[762] Art. 95 de la convention d'application Schengen.
[763] Art. 92 de la convention d'application Schengen.
[764] Art. 93 de la convention d'application Schengen.
[765] Art. 101 de la convention d'application Schengen.

nombre croissant de pays parties à la convention et qu'il était par ailleurs nécessaire de s'adapter aux nouvelles technologies, la refonte du fichier a été décidée[766]. Ainsi, le SIS II vise à assurer une meilleure sécurité en insérant notamment de nouvelles données telles que les données biométriques.

Le règlement (CE) 1987/2006 du 20 décembre 2006[767], la décision 2007/533/JAI du Conseil du 12 juin 2007[768] instaurent la deuxième génération du SIS. Le décret n° 2016-1956 du 28 décembre 2016[769] vient modifier entre autres les dispositions du code de la sécurité intérieure afin d'y codifier les nouvelles dispositions relatives au SIS II. Désormais, le fichier peut contenir des données biométriques ainsi que des données relatives aux interdictions de séjour. Le fichier s'inscrit donc clairement comme un outil répressif et non plus seulement comme un outil d'information. L'accès reste toujours strictement limité aux autorités désignées et l'article 39 du règlement du 20 décembre 2006 précise que les informations contenues ne peuvent être portées à la connaissance de pays tiers.

La convention Schengen reconnait des droits en matière de protection des données personnelles aux personnes signalées dans le SIS[770].

Les accords de Schengen ont posé la base structurelle de la coopération internationale. Il convient toutefois de s'interroger sur la mise en œuvre d'une telle coopération entre des Etats n'étant pas membre de l'espace Schengen et plus encore avec des Etats non membres de l'Union européenne.

B. Le partage de données à caractère personnel avec les Etats n'adhérant pas à Schengen

262. Coopération avec les Etats membres de l'Union européenne n'adhérant pas à la convention Schengen – Il s'agit des régimes dérogatoires applicables aux Etats ayant rejeté l'idée même de l'ouverture des frontières prévue par les accords de Schengen. C'est notamment le cas à l'époque, du Royaume-Uni, de l'Irlande et du Danemark. Ces derniers ont

[766] Règlement (CE) n° 2424/2001 du Conseil du 6 décembre 2001 relatif au développement du système d'information de Schengen de deuxième génération (SIS II) et Décision 2001/886/JAI du Conseil du 6 décembre 2001 relative au développement du système d'information de Schengen de deuxième génération (SIS II).

[767] Règlement (CE) 1987/2006 du Parlement européen et du Conseil du 20 décembre 2006 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen de deuxième génération (SIS II).

[768] Décision 2007/533/JAI du Conseil du 12 juin 2007 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen de deuxième génération (SIS II).

[769] Décret n°2016-1956 du 28 décembre 2016 relatif à la partie nationale du système d'information Schengen de deuxième génération (N-SIS II).

[770] Art. 102 et suivants de la convention d'application Schengen. Voir Partie II.

refusé la suppression des contrôles aux frontières imposant que soit mise en œuvre des régimes particuliers. S'agissant de l'Irlande et du Royaume-Uni (avant le Brexit), une clause *d'opting-in* leur permet de ne mettre en œuvre qu'une partie seulement des dispositions de la convention Schengen. Le Royaume-Uni avait fait le choix de participer en partie à la coopération policière et judiciaire en matière pénale ainsi qu'à l'alimentation du SIS. L'Irlande participe également à l'alimentation du fichier. Ces deux pays participent dans une certaine mesure à la coopération internationale mais n'ont par exemple pas accès aux données visées par l'article 96 de la convention d'application Schengen[771]. Cette clause leur permet de continuer les contrôles aux frontières sur la base de leur législation interne et de ne pas mettre en œuvre systématiquement les dispositions en matière de visas, d'asile et d'immigration décidées dans le cadre de la convention.

Les neuf pays ayant rejoint l'Union européenne en 2004 ont adhéré à l'espace Schengen le 21 décembre 2007. Chypre, la Roumanie, la Croatie et la Bulgarie restent toujours hors de l'espace Schengen.

Les options de retrait (*opting-out*) permettent à certains Etats membres de l'Union européenne ne de pas adhérer à certaines politiques communes et dispositions du droit de l'Union. Il s'agit là aussi d'un système à la carte. Ainsi, le Danemark bénéficie de plusieurs clauses de retrait, notamment s'agissant de la politique de sécurité commune pour laquelle il n'a de ce fait aucun droit décisionnel. Aussi, il possède un droit de retrait en matière de sécurité et de justice tout comme l'Irlande et le Royaume-Uni[772].

La sortie du Royaume-Uni de l'Union européenne pose nécessairement des questions en termes de poursuite de la coopération avec l'Europe notamment s'agissant de son droit d'accès à certaines données du SIS et plus encore à sa participation à Europol. Il est toutefois possible de mettre en œuvre une coopération avec des Etats non membres de l'Union européenne par le biais d'accords comme c'est le cas notamment avec les Etats-Unis.

263. Coopération avec les Etats non membres de l'Union européenne – La coopération avec les Etats non membres de l'Union européenne et qui n'adhèrent pas à Schengen passe nécessairement par la conclusion d'accords comme c'est le cas avec les Etats-Unis par exemple. Ces accords peuvent également être conclus par le biais des agences Europol et

[771] L'article 96 de la convention d'application Schengen vise les données relatives aux individus signalés aux fins de non admission dans l'espace Schengen au motif qu'ils ont été condamnés à une peine privative de liberté d'au moins un an ou qu'ils sont soupçonnés d'avoir commis des faits d'une particulière gravité ou d'envisager de commettre de tels faits.

[772] A noter que la question du passage à un système d'*opting-in* a été soumise à référendum au Danemark le 3 décembre 2015 et a très largement été rejetée par les citoyens.

Eurojust. Sur l'échange de données, il s'agit par exemple des accords dits PNR (*Passenger name record*). Ces accords font suite aux attentats perpétrés le 11 septembre 2001. L'idée est de collecter les données relatives aux passagers aériens lors de leur réservation. Les données visées sont alors très larges puisqu'elles concernent tant les informations relatives à l'identité de la personne (nom, prénom, adresse, téléphone…), qu'à la réservation elle-même (destination, tarif, numéro de siège, numéro des bagages…), au paiement (numéro de carte bancaire…) ou à l'état de santé de l'individu. La liste des données concernées est strictement fixée en annexe de l'accord et compte 19 données[773]. Un accord a été conclu entre l'Union européenne et les Etats-Unis le 8 décembre 2011[774] et approuvé par le Parlement européen le 19 avril 2012[775]. Les données ainsi collectées sont conservées sur une base dite « active » pendant cinq ans puis transférées sur une base « dormante » pour une durée maximum de dix ans. A l'issue d'un délai de six mois, les données sont « dépersonnalisées ».

Aussi, le 30 novembre 2009[776], le Conseil a donné son aval à la signature d'un accord provisoire entre les Etats-Unis et l'Union européenne qui permettrait d'accéder aux données de la société Swift (*Society for worldwide interbank*) traitant des flux financiers. Dans un premier temps, le Parlement européen a rejeté ce projet considérant que les garanties en termes de sécurité des données étaient insuffisantes. Suite à de nouvelles négociations, les accords Swift ont été signés le 28 juin 2010 et adopté le 13 juillet 2010[777]. La finalité de cet accord est clairement la lutte contre le terrorisme et son financement. Lors des débats, le Parlement a néanmoins soulevé certaines inquiétudes notamment quant aux données visées. L'accord fait référence à la transmission de « données potentiellement intéressantes [778]» ainsi qu'aux données « nécessaires[779] ». La question des données à caractère personnel qui

[773] L'annexe de l'accord PNR prévoit que peuvent être collectées les données suivantes : code repère du dossier passager, date de réservation et émission du billet, date du voyage, nom, informations sur les éventuels programme de fidélisation, autres noms figurant dans le dossier passager, toutes les coordonnées disponibles, toutes informations relatives au paiement, itinéraire, agence de voyage, information sur le partage de code, informations PNR scindé/divisé, statut du voyageur, numéro des billets, toutes informations relatives aux bagages, numéro de siège, remarques générales, historique complet des modifications des données PNR.

[774]Accord entre les Etats-Unis d'Amérique et l'Union européenne sur l'utilisation des données des dossiers de passagers (données PNR) et leur transfert au ministère américain de la sécurité intérieure (8 décembre 2011), Conseil de l'Union européenne

[775] Résolution législative du Parlement européen du 19 avril 2012 sur le projet de décision du Conseil relative à la conclusion de l'accord entre les 2tats-Unis et l'Union européenne sur l'utilisation des données des dossiers passagers et leur transfert au ministère américain de la sécurité intérieure (17433/2011-C7-0511/2011-2011/0382(NLE)).

[776] Décision du Conseil 2010/16/PESC/JAI du 30 novembre 2009.

[777] Accords 2010/412/UE du 13 juillet 2010 sur le traitement et le transfert de données de messagerie financière de l'Union européenne aux Etats-Unis aux fins de programme de surveillance du financement du terrorisme.

[778] Accord Swift article 4 point 6.

[779] Accord Swift article 4 point 2.

pourraient être traitées de la même manière lors de ces traitements de masse a été posée[780], l'accord reste assez silencieux sur la question. L'accord prévoit que les données ne pourront être consultées que par les « services répressifs »[781] intervenant en matière de lutte contre le terrorisme. Il peut notamment s'agir d'Interpol.

Un accord similaire avait été conclu entre l'Union européenne et le Canada mais si la CJUE a validé l'idée même de mettre en œuvre un tel système entre ces deux entités, elle a néanmoins rejeté le projet au motif que les garanties en termes de protection des données personnelles n'étaient pas suffisantes[782].

Suite aux attentats perpétrés à Paris en janvier 2015, le Gouvernement français a souhaité instaurer un fichier similaire. Celui-ci a été adopté par le Parlement européen le 14 avril 2016 après plusieurs rejets par la Commission, puis a été finalement adopté en décembre 2015. Les Etats avaient deux ans pour transposer cette directive. La France a intégré ce dispositif au sein de la loi sur la sécurité intérieure du 30 octobre 2017[783]. Il s'agit ici d'un dispositif touchant les Etats membres instauré sur le modèle déjà utilisé entre l'Union européenne et les Etats-Unis.

Le partage de données transfrontières peut aussi relever de la coopération renforcée.

C. Le partage de données à caractère personnel dans le cadre de la coopération renforcée dans l'espace de liberté, de sécurité et de justice

264. Espace de liberté, de sécurité et de justice – La création d'un espace de liberté, de sécurité et de justice (ELSJ) était prévue dès le traité de Rome[784] puis a été consacré dans le traité de Lisbonne du 13 décembre 2007. L'idée d'assurer un niveau élevé de protection pour les ressortissants de l'Union est clairement mentionnée dan l'article 29 du traité de Maastricht[785]. C'est lors du Conseil européen de Tampere en 1999[786] que l'idée de consacrer

[780] Voir à ce sujet, Communication de M. Robert Badinter sur l'accord sur le transfert de données entre l'Union européenne et les États-Unis (SWIFT) du 1er juillet 2010, (https://www.senat.fr/ue/pac/E5430.html). A ce sujet, le Sénat demandait à ce que l'accord prévoit clairement l'exclusion des données sensibles de celles susceptibles d'être transmises dans le cadre de l'accord.

[781] Accord Swift article 1er, 5, 7 et 8.

[782] CJUE, avis 1/15 du 26 juillet 2017. La Cour de justice a considéré que plusieurs dispositions de l'accord méconnaissaient les droits fondamentaux garantis par l'Union, notamment avec les articles 7 et 8.
Voir à ce sujet, Autier E., *La CJUE déclare incompatible l'accord des données PNR signé avec le Canada*, Dalloz actualité 28 juillet 2017. Castets-Renard C., *L'accord PNR UE-Canada : validation conditionnelle par la CJUE*, Dalloz IP/IT 2017, page 420. Communiqué de presse de la CJUE n°84/17 du 26 juillet 2017.

[783] Loi n°2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme.

[784] Art. 61 du traité de Rome du 25 mars 1957.

[785] Art. 29 du traité de Maastricht, « Sans préjudice des compétences de la Communauté européenne, l'objectif de l'Union est d'offrir aux citoyens un niveau élevé de protection dans un espace de liberté, de sécurité et de

un tel espace de sécurité est abordée par les différents chefs d'Etat membres de l'Union. Les lignes directrices qui sont alors définies visent la mise en œuvre d'une politique commune en matière d'asile et d'immigration, la création d'un espace européen de justice, la lutte commune contre la criminalité et le renforcement de l'action extérieure. Le traité de Lisbonne du 17 décembre 2007 marque l'intégration dans le premier pilier de la coopération judiciaire et policière en matière pénale en consacrant en matière pénale ce qui existait déjà en matière civile. L'objectif est de renforcer l'efficacité de la coopération, le pouvoir décisionnel étant désormais dévolu au Conseil des ministres et au Parlement européen. Les décisions relatives à l'espace de liberté, de sécurité et de justice sont désormais prises à la majorité qualifiée des membres du conseil des ministres. Le Parlement dispose d'un pouvoir de codécision. Des mécanismes de coopération renforcée sont mis en œuvre dans certains domaines et notamment en matière de lutte contre le terrorisme.

265. Dispositions renforcées – Le traité prévoit la possibilité pour les Etats qui le souhaitent de prendre des dispositions de coopération renforcée même dans le cas où les autres pays s'y opposeraient, rompant là aussi avec la logique d'uniformisation. Le traité de Lisbonne reprend et renforce en la matière ce qui a été initié par le traité d'Amsterdam. Ainsi, ce type de coopération peut désormais être mise en œuvre dans tous les domaines à la condition qu'elle soit demandée par au moins neuf Etats. Cette coopération doit être autorisée par le Conseil des ministres à la majorité qualifiée, sur proposition de la Commission et après approbation du Parlement européen. Toutefois, en matière de politique étrangère et de sécurité commune (PESC) l'autorisation doit être donnée à l'unanimité. A noter que si un Etat considère que ladite coopération s'oppose aux intérêts fondamentaux qu'il défend il peut renvoyer la proposition devant le Conseil qui cherchera alors à obtenir un consensus. En l'absence de consensus, les neuf Etats pourront recourir à cette coopération actionnant ainsi la clause d'accélérateur[787].

En matière de coopération renforcée, il faut citer le traité de Prüm du 27 mai 2005[788]. Ce traité qui a par la suite été intégré au droit de l'Union européenne par deux décisions du Conseil en

justice, en élaborant une action en commun entre les États membres dans le domaine de la coopération policière et judiciaire en matière pénale, en prévenant le racisme et la xénophobie et en luttant contre ces phénomènes ».

[786] Conseil européen des 15 et 16 octobre 1999, Tampere.

[787] Cette clause n'a pour l'heure jamais été utilisée. Elle peut permettre néanmoins à un certain nombre d'Etats de mettre en place une coopération judiciaire renforcée qui ne serait pas suivi par tous les Etats membres. Voir l'article 20 du traité TFUE 2012.

[788] Traité du 27 mai 2005 relatif au renforcement de la coopération transfrontalière ratifié initialement par l'Allemagne, la Belgique, la France, l'Espagne, le Luxembourg, les Pays-Bas et l'Autriche, et publié par le décret n°2008-33 du 10 janvier 2008.

date du 23 juin 2008[789] a pour objectif la mise en place d'une coopération accrue entre les Etats signataires, notamment en matière de lutte contre la criminalité transfrontalière, en autorisant pour la première fois le partage de données portant sur l'ADN des individus ainsi que sur les empreintes digitales. En donnant accès aux données ADN détenues par les autres Etats signataires, un échantillon ADN non identifié sur le territoire pourrait le devenir en le comparant aux bases de données des autres pays. Ce traité marque une avancée en termes de coopération et de partage de données à caractère personnel au niveau international puisqu'il s'agit de mettre à disposition ces données par un droit d'accès à différents fichiers et registres (notamment le FNAEG, le FAED et le registre des immatriculations de véhicules). En cas de concordances entre les données recueillies par l'Etat demandeur et celles contenues dans le fichier, ce dernier pourra alors obtenir des informations plus précises sur l'individu concerné par le biais de la procédure classique d'entraide judiciaire. L'article 5 de la décision 2008/616/JAI du Conseil qui met en œuvre l'intégration de ce traité au droit de l'Union fait référence à une réelle mise à disposition des données concernées reprenant ainsi certaines des dispositions du programme de La Haye[790]. Les Etats doivent prendre « *toutes les mesures nécessaires pour que la consultation ou la comparaison automatisée de données ADN, de données dactyloscopiques et de données relatives à l'immatriculation de véhicules soit possible 24 heures sur 24 et 7 jours sur 7* ». L'article 14 du traité prévoit également que lors de l'organisation de manifestations de grande envergure, les Etats peuvent sur demande ou spontanément partager des données à caractère personnel avec d'autres Etats relatives à tout individu qui pourrait présenter un danger au vu notamment de ses antécédents. Les données sont transmises au « point de contact » national déterminé par les Etats. De même en matière d'infractions terroristes[791], les Etats peuvent transmettre des données relatives à certains individus de leur propre initiative.

Il convient désormais de s'intéresser aux acteurs mettant en œuvre ce partage de données par le biais des mécanismes de coopération.

[789] Décision du Conseil 2008/615/JAI relative à l'approfondissement de la coopération transfrontalière, notamment en vue de lutter contre le terrorisme et la criminalité transfrontalière et décision du Conseil 2008/616/JAI du 28 juin 2008 concernant la mise en œuvre de la décision 2008/615/JAI relative à l'approfondissement de la coopération transfrontalière, notamment en vue de lutter contre le terrorisme et la criminalité transfrontalière.

[790] Le programme de La Haye du 5 novembre 2004 précise que le partage d'informations est essentiel dans la lutte contre le terrorisme et prévoit dans ses objectifs de trouver « un juste équilibre entre la protection de la vie privée et de la sécurité lors du partage d'informations ».

[791] Il s'agit des infractions visées par les articles 1 à 3 de la décision-cadre du Conseil du 13 juin 2002 relative à la lutte contre le terrorisme.

§2. Les acteurs de la coopération judiciaire et policière

266. Cadre matériel – Il ne semble plus si aisé de traiter séparément la coopération judiciaire et policière tant les textes et accords tendent désormais à les envisager ensemble comme étant complémentaires l'une de l'autre. Néanmoins, dans le cadre d'une étude matérielle, il peut être intéressant d'étudier les deux séparément. Il s'agit ici de s'interroger sur le cadre matériel et sur les différents acteurs intervenant en matière de coopération judiciaire et policière et notamment en matière de partage de données à caractère personnel. Cette étude amène à la conclusion de l'existence d'une multitude d'acteurs intervenant en matière de coopération internationale chacun ayant un rôle bien défini. Il convient donc de s'intéresser aux acteurs de la coopération judiciaires (A.) et policière (B.).

A. Les acteurs de la coopération judiciaire

267. Nombreux acteurs – De manière générale de nombreux acteurs interviennent dans la mise en œuvre et l'encadrement de la coopération judiciaire tels que la Commission européenne, le Parlement et le Conseil ainsi que les parlements nationaux. On peut également citer des organismes créés spécifiquement tel que le comité permanent de coopération opérationnelle en matière de sécurité intérieure (COSI) créé par le traité de Lisbonne et institué par la décision 2010/131/EU du Conseil du 25 février 2010. Son rôle est d'assurer la coordination des différentes orientations décidées par les organismes de l'Union en matière de coopération internationale ainsi que les actions des différents acteurs. L'idée était de créer un comité permanent chargé de cette coordination. De la même manière au niveau national, le bureau d'entraide pénale internationale, composé de magistrats et greffiers, rattaché au ministère de la justice est chargé de la transmission des demandes d'entraide judiciaire.
Il s'agit ici de s'intéresser aux différents acteurs intervenant en matière de coopération judiciaire et plus précisément en matière de partage de données à caractère personnel.

1° Les acteurs du partage de données dans le cadre de la coopération judiciaire

268. Complémentarité des fonctions – Les acteurs intervenant en matière de coopération judiciaire sont nombreux mais leurs missions respectives sont très strictement déterminées de sorte que chacun intervient en complément de l'autre et non en doublon.

269. Magistrats de liaison – Intervenant au niveau national, les magistrats de liaison ont été créés en 1993 à l'initiative de la France. Le premier a été institué en Italie en 1996 avec l'objectif de faciliter la coopération judiciaire entre les deux pays. La décision 96/277/JAI du Conseil en date du 22 avril 1996 définit une action commune en matière d'échange de magistrats de liaison dans le but d'améliorer la coopération judiciaire entre les Etats membres. Ces magistrats ont pour mission de « favoriser et d'accélérer, notamment par l'établissement de contacts directs avec les services compétents et avec les autorités judiciaires de l'Etat d'accueil, toutes les formes de coopération en matière pénale »[792]. Le second paragraphe de l'article prévoit notamment que dans le cadre de ces missions, le magistrat de liaison peut être amené à échanger des informations, données statistiques et des banques de données juridiques. En France une circulaire en date du 14 novembre 1997 est venue préciser les missions de ces magistrats.

270. Les équipes conjointes d'enquête – Ces équipes ont été instituées par la Convention du 29 mai 2000 relative à l'entraide judiciaire pénale et la décision-cadre du 13 juin 2002[793] relative à la lutte contre le terrorisme. Codifié aux articles 695-2 et 695-3 du code de procédure pénale, cette faculté nécessite l'accord préalable du ministre de la Justice ainsi que l'autorité compétente dans le pays respectif. Elle permet alors de créer pour une durée et un dossier limité, une équipe conjointe d'enquête réunissant les magistrats et enquêteurs de deux pays. Dans ce cadre, les deux Etats peuvent échanger les déclarations recueillies et procès-verbaux dressés, de procéder à des opérations de surveillance et d'infiltration sans autorisation préalable. Ce mécanisme relativement souple permet un échange de données assez simple et sans trop de formalités préalables. Néanmoins il faut garder à l'esprit que ces équipes conjointes d'enquête n'ont vocation à intervenir que ponctuellement pour une mission donnée. L'idée est de mutualiser les moyens lorsque sont en jeu des intérêts communs à deux pays.

2° L'unité chargée du renforcement de la coopération judiciaire en Europe : Eurojust

271. Eurojust – L'unité Eurojust est née de la volonté d'aligner la coopération judiciaire sur le modèle de la coopération policière en créant un organisme spécifique visant à renforcer l'efficacité de la coopération. L'unité a été instituée par la décision du Conseil du 28 février

[792] Article 2, action commune du 22 avril 1996, adoptée par le Conseil sur la base de l'article K.3 du traité sur l'Union européenne, concernant un cadre d'échange de magistrats de liaison visant à l'amélioration de la coopération judiciaire entre les États membres de l'Union européenne

[793] Décision-cadre du Conseil 2002/475/JAI du 13 juin 2002 relative à la lutte contre le terrorisme.

2002[794]. Cette décision fait suite au sommet de Tampere des 15 et 16 octobre 1999 et de la volonté de renforcer la coopération en matière d'infractions graves. Ainsi, chaque Etat désigne un représentant. Les missions de ces représentants interviennent en complément de celles du réseau judiciaire européen et des magistrats de liaison et en partenariat avec eux et notamment avec Europol. Pour remplir ces fonctions, l'unité est amenée à traiter des données à caractère personnel par voie automatisée ou non le Conseil prévoyant que soit observé un fort degré de protection s'agissant de ces données[795].

Eurojust intervient principalement en matière de terrorisme, de trafic de drogues, de traite des êtres humains, de fraude, de corruption, de cybercriminalité, de blanchiment d'argent ainsi que d'autres activités liées à la criminalité organisée dans la sphère économique[796]. L'unité n'intervenait initialement que sur saisine des autorités judiciaires nationales. Elle remplit des missions de coordination opérationnelle d'enquêtes ainsi que d'analyse criminelle du renseignement.

Dans ce cadre, l'unité Eurojust est amenée à traiter des données à caractère personnel qui seraient « adéquates, pertinentes et non excessives au regard des fins auxquelles elles sont traitées »[797]. Ces données sont néanmoins strictement définies par le Conseil. Ainsi ne peuvent faire l'objet d'un traitement par Eurojust que les données concernant par exemple l'identité de personnes faisant l'objet d'une enquête ou étant considérées comme témoins ou victimes ainsi que des informations relatives aux faits et aux circonstances de l'infraction ainsi que toutes « informations relatives à l'appartenance présumée à une organisation criminelle »[798]. Ces données recueillies sont stockées dans un fichier temporaire dont seuls les membres autorisés ont un droit d'accès. La décision du 16 décembre 2008[799] est venue renforcer le rôle d'Eurojust et prévoit notamment de faciliter la transmission d'informations à l'unité. A ce sujet une circulaire du 2 août 2011[800] est venue préciser les modalités attachées à cette obligation d'information. Il est ainsi rappelé que lorsqu'est commise une infraction entrant dans le champ de compétence d'Eurojust, le procureur général a une « compétence liée » et doit prendre les mesures utiles et porter dans les plus brefs délais le dossier à la connaissance du représentant national d'Eurojust. Ces missions sont reprises dans le traité de Lisbonne et

[794] Décision 2002/187/JAI du Conseil du 28 février 2002 instituant Eurojust afin de renforcer la lutte contre les formes graves de criminalité.
[795] La décision 2002/187/JAI prévoit la création d'un organe de contrôle indépendant ayant pour mission de s'assurer de la protection des données personnelles.
[796] Art. 4 de la décision 2002/187/JAI.
[797] Art. 14 de la décision 2002/187/JAI.
[798] Art. 15 de la décision 2002/187/JAI.
[799] Décision 2009/426/JAI du Conseil du 16 décembre 2008 sur le renforcement d'Eurojust.
[800] Circulaire du 2 août 2011 portant sur l'obligation d'information de l'Unité Eurojust.

dans le traité TFUE dans sa version consolidée de 2008. Ces textes précisent que l'unité peut désormais prendre l'initiative d'enquêtes pénales, assurer la coordination de ces enquêtes communes, renforcer la coopération judiciaire[801]. C'est à cette époque qu'émerge l'idée de créer un Parquet européen.

272. Vers la création d'un Parquet européen – L'idée de créer un Parquet européen n'est pas nouvelle. Cette dernière émerge très clairement dans le traité de Nice et le traité de Lisbonne. Ainsi, l'article 86 du traité TFUE prévoit la création d'un Parquet européen à partir d'Eurojust visant à lutter contre les fraudes financières[802]. En 1977, le président de la République avait proposé devant le Conseil européen que soit créé un espace judiciaire européen. Cette idée n'avait toutefois pas été retenue comme celle émise en 1982 de créer une Cour pénale européenne. Le sujet a refait surface lors de la création d'Eurojust avec l'idée de créer un procureur européen indépendant. En 2001 la commission européenne se prononce en faveur de la création d'un Parquet européen dans un livre vert[803]. Rappelant les « limites des espaces judiciaires nationaux face à la criminalité économique et financière transnationale »[804], la commission a rappelé l'importance de poursuivre le débat sur la question. Les objectifs sont entre autres de « surmonter le morcellement de l'espace pénal européen »[805], « dépasser le caractère lourd et inadapté des méthodes classiques de la coopération judiciaire entre les États membres »[806] ou « renforcer l'organisation et l'efficacité des recherches à l'intérieur des institutions communautaires »[807]. La Commission soulève notamment la difficulté d'échange d'informations entre les Etats membres entre eux et à destination de l'OLAF dans le cadre des suites judiciaires aux enquêtes administratives rendant parfois des éléments de preuve inadmissibles[808]. Les infractions financières dont il

[801] Art. 85 du traité TFUE version consolidée et article69D du traité de Lisbonne.

[802] Art. 86 al. 1er du traité TFUE version consolidée « Pour combattre les infractions portant atteinte aux intérêts financiers de l'Union, le Conseil, statuant par voie de règlements conformément à une procédure législative spéciale, peut instituer un Parquet européen à partir d'Eurojust. Le Conseil statue à l'unanimité, après approbation du Parlement européen ».

L'idée avait été inscrite dans le traité constitutionnel du 29 octobre 2004 à l'article III-274 qui n'est pas entré en vigueur faute de ratification par tous les Etats membres.

[803] Livre vert sur la protection pénale des intérêts financiers communautaires et la création d'un procureur européen du 11 décembre 2001.

[804] *Ibid*, p. 13.

[805] *Ibid*, p. 14.

[806] *Ibid*, p. 16.

[807] *Ibid*, p. 16.

808 Ce point avait été soulevé lors de la conférence intergouvernementale de Nice. La problématique repose sur les différences de législations entre Etats. L'exemple donné est celui de faits qui relèveraient dans un Etat d'un magistrat et dans un autre d'une autorité administrative ; ces deux entités n'ont pas les mêmes accès aux données notamment du fait de l'application de certaines règles telles que le secret de l'instruction ou le secret des affaires.

question visent essentiellement celles qui portent atteinte au budget de l'Union c'est-à-dire la corruption, le blanchiment et la fraude transfrontalière impliquant des fonds européens. Une des plus importantes visée dans le livre vert est la fraude à la TVA[809].

273. Adoption du Parquet européen – Le 17 juillet 2013, la Commission adopte une proposition de règlement du Conseil portant création du Parquet européen qui n'a toutefois pas retenu l'unanimité de ce dernier. Néanmoins faisant application de l'article 86 du traité TFUE (qui prévoit qu'en l'absence d'unanimité au moins neuf Etats peuvent demander que le Conseil soit saisi du projet), le 3 avril 2017 seize Etats se sont prononcés en faveur de l'instauration d'une coopération renforcée et pour la création d'un Parquet européen[810]. Ainsi est adopté le règlement du 12 octobre 2017[811]. Dans son article 2, il précise différentes notions et notamment celle de données à caractère personnel pour laquelle il reprend la définition désormais admise et précise qu'il s'agit de « toute information se rapportant à une personne physique identifiée ou identifiable »[812]. Le règlement encadre les enquêtes et poursuites diligentées par le Parquet européen. De manière générale, le Parquet européen est organisé en deux échelons, un échelon central et un échelon décentralisé. Au niveau central, le bureau central est composé des chambres permanentes, du collège, du chef de Parquet ainsi que de procureurs européens. Au niveau décentralisé, on trouve des procureurs délégués affectés dans chaque Etat membre[813]. Le règlement précise que la Parquet européen est compétent en

---

Ces difficultés d'échange d'informations posent nécessairement problème lorsqu'il s'agit d'instaurer une coopération.

[809] Avec l'ouverture des frontières et la suppression des contrôles une exonération de taxe s'applique sur les produits exportés. La TVA doit être acquittée dans le pays dans lequel le produit est consommé ce qui n'est pas toujours le cas.

[810] Il s'agit de l'Allemagne, la Belgique, la Bulgarie, Chypre, la Croatie, l'Espagne, la Finlande, la France, la Grèce, la Lituanie, le Luxembourg, le Portugal, la République tchèque, la Roumanie, la Slovaquie et la Slovénie.

[811] Règlement (UE) 2017/1939 du Conseil du 12 octobre 2017 mettant en œuvre une coopération renforcée concernant la création du Parquet européen.

[812] L'article 2 point 7) du règlement du 12 octobre 2017 précise qu' *« 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 »*. Aussi, le point 8) définit le traitement comme *« toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction »*. Le point 12) définit le fichier comme « 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 ».

[813] Art. 8 et suivants du règlement du 12 octobre 2017.

matière d'infractions pénales portant atteinte aux intérêts financiers de l'Union européenne[814] et causant un préjudice de 10000 euros ou plus[815], mais aussi en matière de criminalité organisée telle que définie par la décision-cadre 2008/841/JAI du 24 octobre 2008 dans les cas où il s'agit d'infractions en rapport avec celles fixées par le règlement ou toutes infractions qui seraient « indissociablement liées »[816]. Rappelons que le traité TFUE prévoyant initialement la création du Parquet européen encadrait strictement les compétences matérielles qui pourraient être dévolues à celui-ci et les limitait aux infractions pénales portant atteinte aux intérêts financiers de l'Union. Ainsi, les autorités nationales compétentes doivent sans délai transmettre au Parquet européen toutes les informations nécessaires en lien avec ses compétences. Il s'agit d'informations relatives aux faits, aux victimes et suspects. Les informations sont ainsi vérifiées et enregistrées par le Parquet européen qui décide s'il ouvre ou non une enquête. Le Parquet européen est en mesure d'obtenir d'autres informations qui lui seraient utiles même si elles ne relèvent pas directement d'infractions entrant dans son champ de compétence. Si le Parquet européen décide d'exercer sa compétence, le Parquet national est déchargé de l'affaire.

Dans les cas où l'infraction est passible d'au moins quatre ans d'emprisonnement, le procureur délégué peut ordonner toute mesure d'enquête telle que des perquisitions, production d'objets, production de données informatiques (même cryptées), gel d'instruments ou produits du crime, interception de communications, repérage et traçage d'objets[817]. Les éléments ainsi recueillis sont admissibles devant toutes les juridictions nationales[818]. Le chapitre VII du règlement traité spécifiquement la question des données traitées par le Parquet européen. Ainsi, les procureurs européens délégués ont accès à toutes les données stockées dans les fichiers d'enquêtes nationales et celles détenues par les autorités répressives nationales ou par les autorités publiques ainsi que les données détenues par les organes, organismes et institutions de l'Union[819]. Le Parquet européen utilise un système de gestion des fichiers permettant leur utilisation opérationnelle et la sécurité des données. Lorsque ce dernier décide d'ouvrir une enquête, il crée un fichier qui rassemble toutes les données nécessaires à l'affaire et recueillies auprès des services nationaux, européen ou par ses propres

[814] Telles que définies dans la directive (UE) 2017/1371 du parlement européen et du Conseil du 5 juillet 2017 relative à la lutte contre la fraude portant atteinte aux intérêts financiers de l'Union au moyen du droit pénal.
[815] Le Parquet européen peut être compétent s'agissant d'un préjudice inférieur à 10 000 euros si l'infraction a des répercussions au niveau de l'Union, si des agents ou membres des institutions de l'Union sont soupçonnés d'avoir commis l'infraction. Article 25 du règlement.
[816] Art. 22 du règlement du 12 octobre 2017.
[817] Art. 30 du règlement du 12 octobre 2017.
[818] Art. 37 du règlement du 12 octobre 2017.
[819] Art. 43 du règlement du 12 octobre 2017.

agents. Ce fichier est géré conformément au droit de l'Etat membre auquel est rattaché de procureur délégué. Seul le chef du Parquet européen, ses adjoints, les procureurs délégués ont accès à ces fichiers. Le chapitre VIII du règlement prévoit des dispositions relatives à la protection des données à caractère personnel stockées[820].

La création du Parquet européen a pour vocation la lutte contre les infractions financières ayant des retombées européennes qui sont souvent liées à la criminalité organisée. Toutefois, la question s'est posée des éventuelles compétences en matière de lutte contre le terrorisme. Ce sujet a d'ores et déjà été abordé notamment par Jean-Claude Juncker lors de son discours annuel sur l'état de l'Union européenne du 13 septembre 2017.

274. Consécration en droit interne – En droit interne, la loi du 24 décembre 2020 intègre au code de procédure pénale les dispositions relatives au Parquet européen, insérant un titre X bis. Ainsi les articles 696-108 et suivants du code de procédure pénale transposent les dispositions du règlement et viennent poser le cadre des modalités de fonctionnement du Parquet européen[821].

B. Les acteurs de la coopération policière

275. Nombreux acteurs – La coopération policière a débuté de manière informelle bien avant d'être encadrée par les textes[822]. Disposant aujourd'hui d'un cadre institutionnel strict elle regroupe, comme pour la coopération judiciaire, de nombreux acteurs.

1° Les acteurs nationaux de coopération policière

276. Les offices centraux – Compétents sur le territoire national, les offices centraux regroupent des agents des services de police judicaire, de gendarmerie, des douanes et des services fiscaux. Il s'agit de services spécialisés dans un domaine particulier qui fonctionnent néanmoins tous sur des bases communes[823]. Leur principale mission est entre autres de

[820] Voir Partie II.
[821] Loi n° 2020-1672 du 24 décembre 2020 relative au Parquet européen, à la justice environnementale et à la justice pénale spécialisée.
[822] Au travers notamment du groupe « Trevi » en 1976.
[823] Art. R.15-18 et R.15-22 du code de procédure pénale.

recueillir et exploiter le renseignement. Le décret du 24 janvier 2005[824] dispose que le magistrat peut faire appel aux services centraux lorsque l'enquête nécessite des compétences techniques spécifiques notamment en matière d'investigations internationales. Ces compétences spécifiques renvoient aux différents offices existants comme par exemple l'office central pour la répression du trafic illicite de stupéfiants, l'office central contre le crime organisé ou l'office central de lutte contre la criminalité liée aux technologies de l'information et de la communication[825]. Les informations et données collectées par les services nationaux sont alors transmises aux offices centraux dès lors que le magistrat fait appel à leurs compétences. Les offices centraux intervenants à un niveau plus étendu sont alors plus en mesure d'établir des rapprochements éventuels entre différentes affaires. Le but de ces services est donc de mutualiser les moyens et les compétences sur une enquête en réunissant différents agents de police, gendarmerie et administrations qui sont en mesure de rassembler plus de renseignements et d'en faire une meilleure analyse en centralisant ces informations. Il s'agit donc bien d'une réelle coopération interservices.

277. Les officiers de liaison – Les officiers de liaisons comme les agents des offices centraux rassemblent des agents de police judiciaire et de gendarmerie. Ces derniers sont positionnés à l'étranger et ont un rôle de coordinateur entre la France et l'Etat dans lequel ils interviennent. Ils dépendent de la direction de la coopération internationale (DCI)[826]. Cette direction a un rôle de coopération, de recueil et d'analyse de données intéressant la sécurité de l'Etat. Elle est ainsi chargée de transmettre aux services nationaux compétents les informations dont elle

[824] Décret n°2005-59 du 24 janvier 2005 modifiant le code de procédure pénale et relatif à la police judiciaire ainsi qu'aux offices centraux de police judiciaire relevant de la sous-direction de la police judiciaire de la direction générale de la gendarmerie nationale.

[825] L'article D.8-1 du code de procédure pénale liste les différents services centraux. *« Les offices centraux de police judiciaire relevant des* articles R. 15-18 *et* R. 15-22 *sont les suivants : 1° Office central pour la répression du faux-monnayage ; 2° Office central pour la répression du trafic illicite des stupéfiants ; 3° Office central pour la répression de la traite des êtres humains ; 4° Office central de lutte contre le trafic des biens culturels ; 5° Office central pour la répression de la grande délinquance financière ; 6° Office central pour la répression de l'immigration irrégulière et de l'emploi d'étrangers sans titre de la direction centrale de la police aux frontières ; 7° Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication ; 8° Office central de lutte contre les atteintes à l'environnement et à la santé publique, de la sous-direction de la police judiciaire de la direction générale de la gendarmerie nationale ; 9° Office central de lutte contre la délinquance itinérante, de la sous-direction de la police judiciaire de la direction générale de la gendarmerie nationale ; 10° Office central pour la répression des violences aux personnes ; 11° Office central de lutte contre le travail illégal, de la sous-direction de la police judiciaire de la direction générale de la gendarmerie nationale ; 12° Office central de lutte contre le crime organisé ; 13° Office central de lutte contre la corruption et les infractions financières et fiscales ; 14° Office central de lutte contre les crimes contre l'humanité, les génocides et les crimes de guerre ».*

[826] Créée par le décret n°2010-973 du 27 août 2010 modifiant le décret n° 85-1057 du 2 octobre 1985 modifié relatif à l'organisation de l'administration centrale du ministère de l'intérieur et de la décentralisation.
Voir, O. Beauvallet, Les investigations judiciaires internationales, 1ère ed., Berger-Levrault, pages 217 à 219.

dispose et définit la position commune des organismes nationaux au niveau international. En cela, cette direction a un rôle en termes de coopération technique et institutionnelle[827].

278. Les services interministériels et sous-directions – Il convient de citer certains services interministériels dont le champ d'action est plus étendu mais qui participent également à cette coopération. Le service interministériel d'assistance technique (SIAT) composé d'agents de police judiciaire, de gendarmerie et des douanes relève de la direction centrale de police judiciaire et plus précisément de la sous-direction de la lutte contre la criminalité organisée et de la délinquance financière. La loi du 9 mars 2004[828] et le décret du 21 juillet 2014[829] précisent que ce service peut faire application des dispositions des articles 706-96 et 706-102-1 et 9 du code de procédure pénale qui permettent *« sans le consentement des intéressés, la captation, la fixation, la transmission et l'enregistrement de paroles prononcées par une ou plusieurs personnes à titre privé ou confidentiel, dans des lieux ou véhicules privés ou publics, ou de l'image d'une ou de plusieurs personnes se trouvant dans un lieu privé »*[830]. L'article 706-81 du code de procédure pénale prévoit la possibilité de recourir à des mesures d'infiltration. Les agents de ce service disposent de moyens très étendus en termes de recueil de données.

De la même manière, la sous-direction antiterroriste (SDAT) est spécialisée dans la lutte contre le terrorisme au niveau national et international.

2° Les organismes internationaux de coopération policière

279. L'office de police criminelle facilitant le renseignement : Europol – La création d'Europol trouve ses origines dans le traité de Maastricht. Elle a fait l'objet d'une convention en date du 26 juillet 1995[831] puis par la suite d'une décision du Conseil[832]. Dans le but de développer et garantir la sécurité en Europe, l'office intervient notamment en facilitant l'échange de données et de renseignements utiles à cette mission. Europol est compétent en

[827] Arrêté du 27 décembre 2017 relatif aux missions et à l'organisation de la direction des ressources et des compétences de la police nationale.
[828] Loi n°2004-204 du 9 mars 2004 portant adaptation de la justice aux évolutions de la criminalité (1) dite loi Perben II.
[829] Décret n°2014-827 du 21 juillet 2014 relatif aux missions du service interministériel d'assistance technique et fixant la liste des services, unités ou organismes placés sous l'autorité du ministère de l'intérieur, prévue aux articles 230-36, 706-99 et 706-102-6 du code de procédure pénale.
[830] Art. 706-96 du code de procédure pénale.
[831] Convention du 26 juillet 21995 entrée en vigueur le 1er octobre 1998.
[832] Décision du Conseil 2009/371/JAI du 6 avril 2009 portant création de l'Office européen de police (Europol).

matière de lutte contre la criminalité organisée, le terrorisme et toute forme de criminalité d'une particulière gravité[833] ainsi que pour toute infraction connexe à celles-ci[834]. L'office intervient principalement en matière de traitement d'informations et renseignements. Ainsi, il recueille, stocke, analyse et échange ces données avec les autorités judiciaires compétentes au sein des Etats membres l'idée étant de « faciliter les enquêtes »[835]. Après analyse d'une situation, l'office est en mesure de demander l'ouverture d'une enquête ; en cela, il dispose d'un rôle d'expert et d'assistance des Etats membres. Europol peut être amené à participer aux équipes conjointes d'enquête[836]. Chaque Etat dispose d'une unité nationale présente sur le territoire, chargée de transmettre les informations à l'office central à sa demande ou sur leur propre initiative. Pour mener à bien sa mission, Europol peut coopérer directement avec d'autres services tels qu'Eurojust ou la banque centrale européenne. Le service dispose d'une base de données lui permettant de stocker et consulter les informations qu'il recueille. Il est notamment amené à conclure des accords avec les Etats tiers fixant notamment les modalités relatives à l'échange et au partage de données à caractère personnel[837]. La transmission de données est très encadrée. De manière générale, ces dernières ne peuvent être partagées qu'en cas de réelle nécessité et sous couvert d'un accord de conventionalité conclu entre les deux Etats[838] ou par dérogation lorsque *« la transmission de ces données est absolument nécessaire à la sauvegarde des intérêts essentiels des États membres concernés dans le cadre des objectifs d'Europol ou dans le but de prévenir un danger imminent lié à la criminalité ou à des infractions terroristes »*[839]. Les données transmises par un Etat ne pourront être partagées qu'à la condition que ce dernier ait donné son accord[840] ce qui interdit par principe toute interconnexion avec d'autres bases de données. Enfin, les données fournies par une entité privée ou un particulier ne peuvent être traitées par Europol que si un accord de coopération a

[833] L'annexe de la décision du Conseil du 6 avril 2009 dresse la liste des autres formes d'infractions relevant de la compétence d'Europol : « trafic de stupéfiants, activités illicites de blanchiment d'argent, criminalité liée aux matières nucléaires et radioactives, filière d'immigration clandestine, traite des êtres humains, criminalité liée au trafic de véhicules volés, homicide volontaire, coups et blessures graves, trafic d'organes et de tissus humains, enlèvement, séquestration et prise d'otage, racisme et xénophobie, vol organisé, trafic de biens culturels, y compris les antiquités et les œuvres d'art, escroquerie et fraude, racket et extorsion de fonds, contrefaçon et piratage de produits, falsification de documents administratifs et trafic de faux, faux-monnayage, falsification de moyens de paiement, criminalité informatique, corruption, trafic d'armes, de munitions et d'explosifs, trafic d'espèces animales menacées, trafic d'espèces et d'essences végétales menacées, criminalité au détriment de l'environnement, trafic de substances hormonales et autres facteurs de croissance ».
[834] Art. 4 de la décision du Conseil 2009/371/JAI du 6 avril 2009.
[835] Art. 5 de la décision du Conseil 2009/371/JAI du 6 avril 2009.
[836] Telles que prévues par la décision-cadre 2002/465/JAI du 13 juin 2002 et convention du 29 mai 2000.
[837] Art. 23 de la décision du Conseil 2009/371/JAI du 6 avril 2009.
[838] Art. 23 points 6, 7, de la décision du Conseil 2009/371/JAI du 6 avril 2009.
[839] Art. 23 points 8, de la décision du Conseil 2009/371/JAI du 6 avril 2009.
[840] Art. 24 de la décision du Conseil 2009/371/JAI du 6 avril 2009.

été signé avec l'Etat émetteur ou à défaut si un protocole d'accord sur la transmission d'informations a été conclu[841]. Il va de soi que les données ne sont accessibles qu'à des agents habilités.

280. L'organisation internationale de police criminelle : Interpol – Interpol est certainement l'organisation de coopération policière la plus ancienne et la plus importante. Créée en 1923 suite aux travaux menés en 1914 lors du premier congrès international de police judiciaire qui s'est tenu à Monaco, l'organisation compte aujourd'hui 192 pays. L'organisation est officiellement créée par la résolution du congrès international de police de Vienne du 7 septembre 1923 sous l'appellation de Commission internationale de police criminelle (C.I.P.C.). Elle devient l'organisation internationale de police criminelle – Interpol (O.I.P.C. Interpol) en 1956[842]. Les statuts initiaux ont été fixés lors de l'assemblée générale de Vienne de 1956[843]. L'organisation a pour buts *« d'assurer et de développer l'assistance réciproque la plus large de toutes les autorités de police criminelle, dans le cadre des lois existant dans les différents pays et dans l'esprit de la Déclaration universelle des droits de l'homme »* et *« d'établir et de développer toutes les institutions capables de contribuer efficacement à la prévention et à la répression des infractions de droit commun »*[844]. Interpol intervient dans six domaines : la sûreté publique et le terrorisme, la drogue et les organisations criminelles, le trafic des êtres humains, la criminalité financière, la recherche des fugitifs et la lutte contre la corruption[845]. Son action repose sur l'existence de bureaux centraux nationaux présents sur une grande majorité du territoire ainsi que sur un réseau de communication mondial sécurisé (le I-24/7). Ce réseau permet l'échange de données entre les différents acteurs d'Interpol. L'organisation fonctionne sur la base de notices[846] transmises notamment

[841] Art. 25 et 26 de la décision du Conseil 2009/371/JAI du 6 avril 2009.
[842] L'histoire de l'organisation est très intéressante puisqu'elle trouve ses prémices dans les vœux émis en 1914 par les Etats participant au congrès de Monaco qui visait notamment la création d'un bureau national d'identification ou la création d'un casier central international. En 1926 lors de l'Assemblée générales qui s'est tenue à Berlin, il est proposé que chaque Etat dispose d'un point de contact national placé au sein de la police nationale. Par la suite, les bureaux centraux sont créés. L'organisation évolue et se spécialise en créant des services plus spécialisés (dans le faux monnayage par exemple ou la criminalité). En 1938 toutefois, les nazis prennent possession de l'organisation. Elle sera reconstruite sur l'initiative de la Belgique en 1946 et son siège sera établi à Paris. Elle obtient le statut d'organisation non gouvernementale en 1949 et devient officiellement l'O.I.C.P. Interpol en 1956 après s'être dotée de statuts plus spécifiques et adaptés à sa mission. En 1971, les Nations Unies lui attribuent le statut d'organisation intergouvernementale. En 2009 un représentant de l'organisation est désigné au niveau de l'Union européenne.
[843] Assemblée générale 25e session Vienne, 1956, I/CONS/GA/1956 (2017).
[844] Art. 2 des statuts fixés lors de l'assemblée générale 25e session Vienne, 1956.
[845] O. BEAUVALLET, Les investigations judiciaires internationales, *op. cit.*, pages 238.
[846] Les notices rouges servent à demander l'arrestation provisoire d'un individu en vue de son extradition ; les notices bleues servent au recueil d'informations complémentaires ; les notices vertes sont utilisées pour alerter et transmettre des informations policières relatives à un individu susceptible de récidiver ; les notices jaunes sont

par les bureaux centraux à destination de tous les acteurs autorisés à y accéder. Dans certains cas certaines informations peuvent être accessibles aux particuliers, par exemple quand Interpol recherche un individu et que ses recherches restent infructueuses. Ces notices contiennent des informations permettant l'identification des individus (état civil, signalement, photographie) et des éléments relatifs aux infractions concernées. Interpol constitue ainsi des bases de données qui sont accessibles par les bureaux centraux nationaux. Il s'agit par exemple de la base de données nominative relative aux individus signalés ou recherchés, la base des empreintes digitales dans laquelle Interpol stocke toutes les traces recueillies ou la base des empreintes génétiques alimentée par les Etats. Le fonctionnement d'Interpol est encadré par de nombreux règlements et amendements et notamment des règlements qui encadrent l'échange de données.

281. L'échange de données via Interpol – Il faut citer la résolution AG/2011/RES/07 du 30 juin 2012 approuvant le règlement relatif au traitement des données qui abroge le Règlement sur le traitement d'informations pour la coopération policière internationale, le Règlement d'application du Règlement sur le traitement d'informations pour la coopération policière internationale et le Règlement portant sur l'accès au réseau de télécommunications et aux bases de données d'INTERPOL par une organisation intergouvernementale. Ce règlement encadre entre autres le traitement des données et la création de bases de données au sein d'Interpol. S'agissant de la création d'une base de données, l'article 29 soumet à approbation du comité exécutif tout projet en la matière. Toute création est ensuite immédiatement notifiée aux bureaux centraux nationaux. Le secrétariat général tient à jour un registre qui recense les bases de données de police d'Interpol[847]. Il appartient aux bureaux centraux ou aux entités nationales ou internationales compétentes d'enregistrer dans la base de données toute information à la condition qu'elle présente un *« intérêt pour la coopération internationale »*[848]. De manière générale, toutes les bases de données d'Interpol voient leur statut juridique déterminé en fonction de ces caractéristiques et notamment leur finalité, la nature des données stockées, les sources d'alimentation, le niveau de confidentialité, les

utilisées pour retrouver des personnes disparues ; les notices noires sont utilisées afin d'obtenir des informations sur une personne décédée et non identifiée ; les notices oranges sont utilisées pour alerter la police et organismes publics sur les menaces pour la sécurité publique ; les notices mauves servent à diffuser des informations relatives aux modes opératoires et enfin les notices spéciales visent à alerter les services de police sur des individus ou groupes visés par des sanctions de l'ONU en matière de terrorisme.

[847] Art. 33 du règlement d'Interpol sur le traitement des données.

[848] Art. 35 du règlement d'Interpol sur le traitement des données.

modalités d'enregistrement de consultation et d'utilisation[849]. Les conditions permettant l'enregistrement des données sont définies au cas par cas mais elles doivent comporter l'identité de la source des données, la date d'enregistrement, la finalité de l'enregistrement, le niveau de confidentialité, le statut de la personne s'agissant des données à caractère personnel, le niveau de confidentialité, les restrictions d'accès[850]. Des conditions supplémentaires sont fixées s'agissant notamment des données sensibles, qui ne peuvent être enregistrées que si elles présentent un caractère pertinent, ont une *« valeur criminalistique particulièrement importante »* et sont objectives[851]. L'article 55 du règlement dispose que toute interconnexion doit répondre à des conditions cumulatives. Ainsi, la finalité et la nature de l'interconnexion doivent être déterminées, l'interconnexion doit présenter un intérêt pour la coopération internationale et donner un niveau de sécurité suffisant « au moins équivalent à celui du système d'information d'Interpol »[852]. Dans le cas où un bureau central ou une entité nationale ou internationale veut utiliser des données à des fins autres que celles initialement fixées, il doit s'assurer que cela n'est pas en contradiction avec la finalité initiale et est licite[853]. Aussi l'utilisation de ces données à des fins administratives nécessite l'autorisation de la source des données[854].

Conclusion du titre 2

282. La multiplication du nombre de fichiers intervenant dans les procédures – Collectées comme potentielles données probatoires dans une procédure, les données à caractère personnel font parfois l'objet d'un fichage au sein de ce que l'on nomme de manière générique des « fichiers judiciaire ». Le premier constat qui peut être fait est celui de la multiplication exponentielle du nombre de fichiers de police existants. Les évolutions technologiques et les évolutions de la criminalité ont conduit à la création de nouveaux fichiers. En ce sens, on ne peut nier les avancées considérables rendues possibles par le fichage ADN. Aussi, la progression de crimes et délits graves ont imposé de repenser les moyens de lutte comme en matière de terrorisme par exemple. Enfin, le développement

[849] Art. 36 du règlement d'Interpol sur le traitement des données.
[850] Art. 37 du règlement d'Interpol sur le traitement des données.
[851] Art. 38 et 42 du règlement d'Interpol sur le traitement des données.
[852] Art. 55 du règlement d'Interpol sur le traitement des données.
[853] Art. 64 du règlement d'Interpol sur le traitement des données.
[854] Art. 65 du règlement d'Interpol sur le traitement des données.

d'internet a constitué à la fois le terrain de nouvelles formes de criminalités mais aussi un nouveau moyen d'action contre celles-ci.

283. Un fichage nécessaire – Face au développement du nombre de fichiers judicaires existants, il faut admettre les avancées rendues possibles en termes de lutte contre les infractions du fait de ces derniers. C'est notamment en termes d'identification des auteurs d'infractions que les avancées ont été les plus remarquables. La conservation de données et traces génétiques et biométriques au sein de fichiers permet sans nul doute de confondre des auteurs d'infractions parfois même des années plus tard. Aussi, l'existence du casier judiciaire national en ce qu'il constitue la mémoire judiciaire permet que les peines prononcées soient adaptées et individualisées et de la même manière constitue un moyen de lutte contre la récidive.

284. Un fichage alarmant – Bien qu'apparaissant nécessaire à la bonne administration de la justice, les fichiers judiciaires soulèvent des interrogations légitimes. La première interrogation porte tout d'abord sur les individus visés par le fichage. Si l'idée d'un fichage des individus suspects ou condamnés dans une procédure apparait légitime, la question du fichage des victimes ou tiers à la procédure inquiète et interroge. La crainte repose sur la question du fichage massif des individus, qui pourrait, dans un certain sens, nuire à l'utilité même des fichiers. Ensuite, les fichiers soulèvent la question de la protection des données qu'ils contiennent. Avec des fichiers contenant de plus en plus de données et des accès de plus en plus ouverts, on peut s'interroger sur la sécurité des données susceptibles d'être partagées et aussi sur la finalité de celles-ci au vu notamment du principe de finalité posé par les textes encadrant le traitement de données. Finalement ce n'est pas nécessairement la question de la création du ficher qui inquiète mais davantage celle de l'utilisation qui en est faite et des répercussions possibles sur les droits et libertés individuels.

285. Nécessaires contrôle sur les fichiers – Face à ces craintes, il apparait alors nécessaire qu'un contrôle effectif soit opéré sur les fichiers dès leur création mais aussi dans leur mise en œuvre. De manière générale, la CNIL a vu ses attributions *a priori* restreintes et si elle est amenée à rendre un avis s'agissant du traitement de données sensibles, on peut regretter que ces derniers ne soient pas toujours suivis d'effets. Le risque majeur réside dans le fait qu'un fichier autorisé peut voir ses finalités modifiées par la suite.

La création et le recours aux fichiers de police doit opérer une délicate mise en balance d'intérêts antagonistes entre notamment la bonne administration de la justice et le respect des droits et libertés individuels auxquels s'ajoute la protection des données à caractère personnel. Cet équilibre appelle la mise en œuvre d'un cadre strict et de contrôles effectifs.

Conclusion de la partie 1

286. La nécessaire exploitation de données personnelles au cours de la procédure – Le premier constat qui doit être fait est celui de la nécessaire exploitation des données personnelles au cours de la procédure. Cette nécessité tient dans l'évidence selon laquelle grand nombre des informations traitées dans une procédure constituent, au sens de la loi informatique et libertés, des données à caractère personnel. Au-delà de cette évidence, il apparait que le traitement de données personnelles est utile et nécessaire à toute action civile ou pénale afin de justifier son action et apporter des preuves. Le fichage soulève évidemment des interrogations en termes de droits et libertés. Néanmoins, celui-ci est nécessaire et certains fichiers ont permis des avancées considérables. C'est évidement la matière pénale qui trouve le plus à les utiliser. Il est évident, que la conservation de données à vocation probatoire permet de résoudre des affaires ou d'identifier des individus, ce qui ne serait pas possible sans ce fichage. Ce constat d'un nécessaire fichage ne doit néanmoins pas occulter les éventuelles atteintes qui peuvent être engendrées par la conservation massive de données notamment lorsque celles-ci constituent des données sensibles.

287. Les données sensibles nécessaires aux procédures – Le déroulement de la procédure nécessite le traitement de données sensibles puisque précisément celles-ci touchent à l'identité de la personne, ce qui renvoie aux procédures visant à prouver la filiation, identifier un auteur, par exemple. Ce traitement de données sensibles apparait donc nécessaire et justifié. Il a été rendu possible par différentes avancées technologiques qui ont permis le recours à de nouvelles données et preuves dans le procès.

Que ce soit en matière civile ou pénale, le constat est celui d'une collecte de données facilitée par les nouveaux moyens technologiques et scientifiques. Leur utilité avérée ne doit toutefois pas aboutir à une utilisation excessive au vu des droits et libertés des individus et nécessite un encadrement strict et un contrôle effectif. Le recours à des procédés qui permettent une collecte massive de données parfois sensibles, tel que les IMSI-catcher ou l'usage des drones, doit nécessairement s'accompagner de garanties adéquates. On peut regretter que le recours à une analyse d'impact ne soit pas toujours effectif et plus encore que les avis de la CNIL sur les projets de mise en œuvre de traitement ne soient pas toujours entendus.

De manière générale, l'extension des procédures relevant de régime dérogatoires doit être observée avec prudence au vu des risques pour les libertés.

Si le Conseil constitutionnel est garant de celles-ci il faut noter que les saisines sont résiduelles sur ces questions. De manière générale, les contrôles opérés sur les textes portant création de fichiers invalident rarement ces derniers.

288. La nécessaire application des principes du droit de la preuve fonction de la nature des données – Il apparait nécessaire de porter une attention particulière en fonction de la nature des données traitées. Si la collecte de données probatoires doit répondre à la double exigence de légalité et de loyauté, certaines données sensibles soulèvent des interrogations particulières de fait de leur nature. Aussi, l'utilisation faite des données de manière générale doit garantir à la fois le respect des principes directeurs du procès et le respect des droits des individus quant au traitement de leurs données.

289. La nécessaire prudence quant aux risques attachés aux interconnexions – S'agissant des données faisant l'objet d'un fichage, si la création est encadrée par les textes et que les traitements portant sur des données sensibles sont soumis à l'aval du Conseil d'Etat, c'est davantage l'utilisation des données qui pose question. La CNIL soulève régulièrement des interrogations liées au transfert de données et plus précisément aux interconnexions entre fichiers. Bien que le texte portant création du fichier doive fixer les finalités précises pour lesquelles les données sont conservées, la CNIL suggère que les potentielles interconnexions soient clairement précisées. En effet, le mécanisme d'interconnexion de fichiers entre eux, s'il a pu être présenté comme une garantie de mis à jour des données, représente au risque majeur quant aux droits des individus. Cette question du transfert de données se pose également s'agissant de l'échange possible de données entre judiciaire et renseignement.

290. L'équilibre entre développement de traitements nécessaires et libertés individuelles – Finalement, il convient d'admettre que la collecte de données et son fichage au sein de fichiers judiciaires constitue une avancée dans le fonctionnement de la justice. Néanmoins, les nouveaux procédés permettent la collecte de données de plus en plus importantes et notamment de données sensibles. Si cela s'accompagne de lois qui élargissent les faits justifiants la collecte et le fichage et ouvre ces données à grand nombre de destinataires, cela laisse planer des doutes quant aux éventuels risques pour les individus.
Il importe de trouver le juste équilibre entre la collecte et le fichage nécessaires et les garanties pour les individus s'agissant de leurs libertés individuelles.

De manière générale, faut-il regretter la suppression du régime d'autorisation de la CNIL ? Celle-ci s'est accompagné de nouveaux moyens de sanctions qui devront néanmoins être effectives afin d'assurer la protection des données personnelles des individus.

DEUXIEME PARTIE

LA PROTECTION DES DONNEES A CARACTERE PERSONNEL DANS LES PROCEDURES JUDICIAIRES

291. Des données intervenant à différents stade de la procédure – Les données intervenant au cours de procédures judiciaires font l'objet de différents traitements. L'obligation générale d'assurer la protection de ces données prend alors différentes formes.

Les données font l'objet de diffusions, par l'application de divers principes, à divers individus. Cette diffusion peut découler de l'application de principes généraux, s'agissant notamment du respect du contradictoire qui impose une communication des pièces versées au dossier à toutes les parties. De plus, les données peuvent être diffusées par l'application du principe de publicité de la justice avec une diffusion cette fois plus large, et d'autant plus avec la mise en *open data* rendue possible par la loi du 23 mars 2019.

La diffusion de données issues de procédures n'a donc pas la même ampleur en fonction de la norme sur laquelle elle repose. Il peut donc s'agir d'une diffusion entre les parties à la procédure ou d'une diffusion plus large par l'application du droit d'accès aux décisions et de leur mise en *open data*.

Il s'agit donc de s'interroger sur la diffusion de ces données aux différents stades de la procédure qui soulève des interrogations différentes attachées notamment à la portée de celle-ci.

292. Une protection assurée par le secret – Quel que soit les dispositions permettant ou imposant la diffusion des données de procédure, celles-ci font l'objet de mesures protectrices. Cette protection peut être nécessaire en fonction du stade de la procédure. C'est ainsi que les données d'enquêtes ou d'instructions en cours sont couvertes par le principe de secret justifié notamment par les nécessités d'une bonne administration de la justice. Les données peuvent aussi être protégées au vu de leur nature comme par exemple s'agissant des données couvertes par le secret professionnel. Enfin, cette protection passe par l'application de procédés d'occultation de certaines données. Il peut s'agir d'occulter l'identité de celui qui révèle des informations comme en matière de témoignage anonyme notamment, ou d'occulter certaines données identifiantes lors de la diffusion des décisions de justice. De manière générale, se sont les conséquences négatives que pourraient avoir la révélation qui justifient la mise en

œuvre de divers principes et procédés. Toutefois, malgré le secret, la divulgation de données peut être nécessaire ou obligatoire. Cette divulgation est alors strictement encadrée.

293. Une protection assurée par l'affirmation de normes encadrant la gestion des données – Les principes qui encadrent le traitement de données assurent la protection de celles-ci notamment en fixant les dispositions relatives à la licéité du traitement et posant des obligations pour les responsables. En matière de données traitées au cours de procédures judiciaires, cela se traduit notamment par l'application des normes régissant la gestion des données fichées. Tout traitement de données doit être nécessaire et proportionné à la finalité qu'il poursuit. Aussi, le responsable du traitement a une obligation de contrôle sur la véracité des données traitées imposant une mise à jour de celles-ci. En conséquence, toute données qui ne seraient plus exactes ou dont le traitement ne serait plus nécessaire doit entrainer la rectification ou l'effacement de celles-ci d'office.

294. Une protection assurée par l'affirmation de droits pour les individus – Cette protection des données issues de procédure passe aussi par l'affirmation de droits pour les individus concernés par un traitement. Ces droits ont été rappelé et accentués avec l'adoption du règlement général sur la protection des données et la loi informatique et libertés et tendent à donner un droit de regard et d'action des individus sur leurs données, que ce soit par l'exercice du droit de rectification, d'opposition ou d'effacement auprès du responsable du traitement. L'effectivité de ces droits nécessite que leur méconnaissance soit sanctionnée. En ce sens, la CNIL a vu ses pouvoirs accentués.
Néanmoins, l'exercice de ces droits peut s'avérer délicat s'agissant des données diffusées sur internet.

295. Problématiques – Le sujet amène à s'interroger sur les dispositions qui permettent une protection des données à caractère personnel intervenant dans une procédure judiciaire. Les enjeux ne sont alors pas les même suivant le stade de la procédure et la portée de la diffusion. Face à la nécessaire diffusion des données de procédures, il faut s'intéresser aux différentes normes qui tendent à assurer une protection de celles-ci et s'interroger sur leur effectivité. Cette question renvoie nécessairement à celle du droit à l'oubli.
Il convient donc de s'intéresser aux principes encadrant la diffusion des données à caractère personnel au cours de la procédure judiciaire (Titre 1), pour appréhender ensuite le sort des données collectées dans le cadre de ces procédures (Titre 2).

TITRE PREMIER

LES PRINCIPES ENCADRANT LA DIFFUSION DES DONNEES A CARACTERE PERSONNEL AU COURS DE LA PROCEDURE JUDICIAIRE

296. La diffusion des données de procédure entre publicité et secret – Au cours d'une procédure judiciaire, de nombreuses données interviennent à différents stades et pour diverses finalités. Certaines de ces données versées au dossier en tant que données informatives ou à vocation probatoire constituent des données à caractère personnel en ce qu'elles permettent l'identification d'un individu. De manière générale, certaines données de la procédure font l'objet d'un régime de protection particulier, c'est le cas des données issues de l'enquête ou de l'instruction qui sont soumises au principe du secret durant la durée de celles-ci. Ainsi, certaines données initialement couvertes par un secret peuvent être amenées à être communiquées. A contrario, certaines données, par principe publiques, peuvent être rendues secrètes.

Cette diffusion des données ne répond pas à des principes liés à la nature personnelle de celles-ci mais est soumise aux règles applicables en matière processuelle. Ainsi, du fait de l'application de ces principes, certaines données sont amenées à être diffusées ou au contraire à ne pas l'être. Il s'agit donc de s'interroger sur les normes qui s'appliquent en matière de diffusion des données en cours de procédure en portant un regard particulier du fait de leur caractère personnel.

Plusieurs intérêts antagonistes s'opposent, soulevant d'un coté la question d'un droit d'accès aux données et d'un autre coté celle de la protection de ces données. Il convient donc dans un premier temps d'envisager les principes limitant la diffusion de données (Chap.1) pour ensuite s'intéresser aux principes justifiant cette diffusion (Chap.2).

CHAPITRE 1 : LES PRINCIPES LIMITANT LA DIFFUSION DE DONNEES

297. Les données de procédure couvertes par un secret – En la procédure civile comme pénale, les données traitées peuvent être protégées par un secret qui nécessite de s'interroger sur les règles applicables en termes de diffusion de celles-ci. En matière pénale, plus précisément, on oppose souvent la phase d'enquête et d'instruction à la phase de jugement. Si le principe du secret semble affirmé lors de l'enquête, son application au cours de l'instruction soulève davantage d'interrogations amenant certains auteurs à le qualifier de « secret de polichinelle »[855]. Si la phase de jugement est par principe publique en matière civile come pénale, une exigence de confidentialité qui tend parfois à s'appliquer contribue directement ou indirectement à assurer une protection des données. En effet, le secret est affirmé lors de la phase d'enquête et d'instruction (Sect.1) alors que dans la phase de jugement s'applique une confidentialité relative (Sect.2).

Section 1 : Un secret affirmé lors de la phase d'enquête et d'instruction

298. Données d'enquête et d'instruction – Au cours de la phase d'enquête ou d'instruction, la règle du secret domine. Ainsi, le principe de secret de l'enquête et de l'instruction impose de taire les informations découvertes lors de la procédure dont certaines constituent des données à caractère personnel. Le principe de protection des données de l'enquête et de l'instruction n'a pas vocation exclusive à protéger les données personnelles. Néanmoins, les données à caractère personnel de la procédure bénéficient de cette protection en tant que données de procédure. Il convient donc de s'y intéresser. Malgré l'affirmation d'un secret protégeant les données de l'enquête et de l'instruction (§1.), on peut reconnaitre l'existence d'un secret partagé applicable aux données des procédures judiciaires (§2.). La prédominance de ce secret se mesure aussi par l'existence d'incriminations spécifiques sanctionnant la communication illégale des données d'enquête et d'instruction (§3.).

[855] Voir à ce sujet, C. Ambroise-Casterot, C. Combeau, La procédure pénale dans la balance : entre secret et transparence, *Les cahiers de la justice*, 2014, p. 373. Les auteures font ici référence au trois phases de la procédure mentionnant une « prédominance » du secret au cours de l'enquête, qualifiant ensuite le secret de « polichinelle » lors de l'instruction et abordant « l'effacement » du secret lors de l'instance.

§1. Le secret protégeant les données de l'enquête et de l'instruction

299. Principe fondamental limité – Erigé en principe fondamental de la procédure pénale, le secret de l'enquête et de l'instruction soulève des interrogations notamment à l'heure où se développe l'idée d'un droit à l'information. Malgré l'affirmation d'un principe protecteur des données (A.), ce dernier a toutefois une portée limitée (B.).

A. L'affirmation d'un principe protecteur des données

300. Un principe fondateur de la procédure pénale – Le secret de l'enquête et de l'instruction est un principe fondateur de la procédure pénale inquisitoire[856]. Dans le système actuel qualifié de mixte, le code de procédure pénale de 1958, consacre le principe de secret de l'enquête et de l'instruction à l'actuel article 11 qui dispose que *« Sauf dans le cas où la loi en dispose autrement et sans préjudice des droits de la défense, la procédure au cours de l'enquête et de l'instruction est secrète. Toute personne qui concourt à cette procédure est tenue au secret professionnel dans les conditions et sous les peines des articles 226-13 et 226-14 du code pénal »*. Le principe du secret de l'enquête et de l'instruction vise à garantir l'efficacité des investigations, à protéger les différents acteurs de la procédure en garantissant notamment la présomption d'innocence et à préserver l'ordre public[857].

301. Un principe doté d'une double fonction – Le Conseil constitutionnel a apporté des précisions sur le sujet à l'occasion d'une question prioritaire de constitutionnalité[858]. Saisi par le Conseil d'Etat, le Conseil constitutionnel a considéré que le secret de l'enquête poursuit à la fois un objectif de garantie d'efficacité des procédures et de protection des personnes (protégeant à la fois leur vie privée et garantissant le respect de la présomption d'innocence). Le Conseil constitutionnel rejoint, sur ce point, la position de la Cour européenne des droits de l'homme qui a rappelé que le secret de l'instruction tend à protéger la vie privée des parties

[856] Le principe est issu de plusieurs textes. L'ordonnance de Blois de 1498 posait une obligation de discrétion quant à la tenue du procès. Plus tard, l'ordonnance de Villers-Cotterets de 1539 a posé les bases du huis-clos s'agissant de certaines affaires. Ensuite, l'ordonnance criminelle du 26 aout 1670 posera l'interdiction pour les greffiers de divulguer les informations dont ils ont eu connaissance du fait de leurs fonctions.
Voir sur la question le rapport d'information de l'Assemblée Nationale n°2540 déposé le 18 décembre 2019 relatif au secret de l'enquête et de l'instruction.

[857] S. Guinchard, J. Buisson, *Procédure pénale*, *op. cit*, p. 1026 et s. J. Larguier, Le secret de l'instruction et l'article 11 du CPP, *RSC* 1959, 313. C. Ambroise Castérot, Droits de la défense et secret de l'instruction, *in*, Guinchard, *Justice et droit du procès*, Dalloz, 2010, p. 887 et s.

[858] Cons. Const., décision n°-693 QPC, 2 mars 2018, Association de la presse judiciaire.

et les intérêts de la justice, renvoyant directement au principe de présomption d'innocence visé à l'article 6 de la Convention européenne des droits de l'homme[859]. A ce sujet, la Cour de cassation a pu, à de nombreuses reprises, confirmer la nécessité de protéger le secret de l'enquête et de l'instruction, le plaçant parfois au dessus de la liberté d'expression et affirmant ainsi l'importance et la portée du principe[860]. Elle a par exemple pu préciser que le fait de divulguer des informations relatives à une information judiciaire en cours constitue un délit quand bien même les éléments révélés auraient déjà été rendus publics[861]. Le principe du secret de l'enquête et de l'instruction se révèle complexe de par cette double vocation. D'un côté, il est garant de la bonne administration de la justice allant dans le sens de l'intérêt général, de l'autre, il protège la vie privée et la présomption d'innocence et défend ainsi des intérêts privés. Le principe du secret de l'enquête et de l'instruction garant du bon déroulement de la procédure soulève plusieurs interrogations tant sur sa portée que sur son application dans la pratique, qu'il est intéressant de mettre en parallèle avec les normes encadrant le traitement de données à caractère personnel.

302. Un principe protégeant l'ensemble des données collectées lors de la procédure – Le principe de secret de l'enquête et de l'instruction s'applique à toutes les données collectées à l'occasion de la procédure et peu importe leur nature. La Cour de cassation a eu l'occasion de préciser cela en affirmant la constitution du délit de violation du secret par la divulgation de données qu'elles soient identifiantes ou non par le seul fait que cette information issue de l'enquête n'est connue que par les enquêteurs[862]. On dépasse donc ici le cadre des données à caractère personnel défini par la loi informatique et liberté de 1978 qui vise les données identifiantes. En ce sens, dans son rapport du 18 décembre 2019, l'Assemblée nationale précise que le secret s'applique, par principe, « à tous les éléments de la procédure »[863].

[859] Cour E.D.H., 14 juin 2005, n°39553/02, *Menet c/ France*, cons. 50. En l'espèce, le requérant invoquait une violation des droits de la défense n'ayant pu accéder au dossier d'instruction. Ce droit lui avait été refusé puisqu'il avait fait le choix de ne pas être représenté par un avocat. La Cour E.D.H. constate en effet que ce choix offert à la partie civile influe sur l'accès ou non au dossier d'instruction. Toutefois, elle rappelle que sans méconnaitre le principe d'égalité des armes, les droits du prévenu et ceux de la partie civile peuvent être « différenciés » (cons. 47). Aussi, elle rappelle que contrairement aux parties, l'avocat est soumis au secret professionnel. Le seul accès au dossier par l'avocat garantit donc le secret de l'instruction (cons. 49).
[860] Voir par exemple pour un arrêt récent en matière de secret de l'enquête, Cass., crim., 24 mars 2020, *pourvoi* n° 19-80.909.
[861] Cass., crim., 7 mars 1989, *pourvoi* n° 87-90.500, *Bull.* crim., n° 109.
[862] Cass. Crim., 24 mars 2020, *pourvoi* n° 19-80.909.
[863] Rapport de la commission des lois, n°2540, 18 décembre 2019, le secret de l'enquête et de l'instruction.

B. La portée limitée du principe du secret de l'enquête et de l'instruction

303. Portée limitée – Bien qu'affirmé strictement, le principe du secret de l'enquête et de l'instruction n'est pas pour autant un principe absolu (1°), la procédure rendant nécessaire la communication de données du dossier aux parties (2°).

1° Un principe non absolu

304. La portée de l'article 11 du code de procédure pénale – La lecture de l'article 11 du code de procédure pénale permet immédiatement de comprendre les limites du principe du secret de l'enquête et de l'instruction et son caractère non absolu. D'abord, si l'on observe la lettre de l'article 11 du code de procédure pénale, ce dernier pose le principe du secret de l'enquête et de l'instruction pour les personnes qui « concourent » à la procédure[864]. Il ne s'agit donc pas d'un principe général dans le sens où il ne vise pas tous les individus[865]. Cette notion renvoie à un secret professionnel tel que visé dans les articles 226-13 et 226-14 du code pénal. Ainsi concourent à la procédure les magistrats, les greffiers, les officiers de police judiciaire[866] ainsi que tout expert et personnes qualifiées requises au cours de la procédure. La Cour de cassation a rappelé dans un arrêt 24 mars 2020 que les fonctionnaires de police concurrent à la procédure et sont donc soumis au secret de l'enquête et de l'instruction. Elle rappelle ainsi une jurisprudence antérieure du 26 octobre 1995 dans laquelle elle avait précisé que les fonctionnaires de police sont soumis au secret s'agissant des données dont ils ont connaissance dans l'exercice de leurs fonctions et qui revêtent un caractère confidentiel[867]. Dans l'arrêt du 24 mars 2020 la Cour de cassation a précisé que viole le secret de l'enquête le fonctionnaire de police qui divulgue une donnée dont seuls les enquêteurs avaient connaissance, peu importe que cette donnée soit identifiante ou non[868].

[864] Art. 11 al. 2 du code de procédure pénale.
[865] Ce caractère non absolu a pu être rappelé à de nombreuses reprises notamment dans un rapport d'information de l'Assemblée nationale en date du 18 décembre 2019 relatif au secret de l'enquête et de l'instruction. La Commission des lois rappelle que le secret de l'enquête s'applique par principe « à tous les éléments de la procédure » mais qu'il n'est « ni général ni absolu ». Rapport de la commission des lois, n°2540, 18 décembre 2019, le secret de l'enquête et de l'instruction, *op. cit.*, p.5. Auditionnée par les rapporteurs, Mme Bouglé - Le Roux (historienne en droit) rappelle que l'article 110 de l'ordonnance de Blois disposait déjà en 1498 que « le procès se fera le plus diligemment et secrètement que faire se pourra », posant ainsi une obligation de moyen et non de résultat. Elle ajoute que « le secret n'est pas un impératif inconditionnel et demeure soumis aux aléas de l'affaire ». Auditionné par la Commission, M. Pers, doyen de la chambre criminelle de la Cour de cassation a rappelé que « le secret de l'enquête et de l'instruction n'est ni général ni absolu » au sens de l'article 11.
[866] Et les agents de police judiciaire.
[867] Cass. crim., 26 octobre 1995, *pourvoi* n°94-84.858.
[868] Cass. Crim., 24 mars 2020, *pourvoi* n° 19-80.909. Ainsi, le fonctionnaire de police qui soumet à un journaliste des informations issues de la procédure en cours viole le secret professionnel. P. J. Delage, Secret de

305. Ne concourent pas à la procédure – En revanche, les avocats ne sont pas soumis au secret de l'enquête et de l'instruction tout comme les parties civiles[869], les personnes mises en cause ou les témoins. L'article 5 du décret du 12 juillet 2005 relatif aux règles de déontologie de la profession d'avocat impose toutefois déontologiquement le respect du secret édicté à l'article 11 sauf dans le cadre de l'exercice des droits de la défense[870]. Cet article dispose que *« L'avocat respecte le secret de l'enquête et de l'instruction en matière pénale, en s'abstenant de communiquer, sauf pour l'exercice des droits de la défense, des renseignements extraits du dossier, ou de publier des documents, pièces ou lettres intéressant une enquête ou une information en cours. Il ne peut transmettre de copies de pièces ou actes du dossier de la procédure à son client ou à des tiers que dans les conditions prévues à l'article 114 du code de procédure pénale »*[871].

306. Un principe qui connait des aménagements – Le principe du secret de l'enquête et de l'instruction connait des limites qui peuvent prendre différentes formes. Ainsi, d'autres règles et principes procéduraux peuvent constituer des limites au principe. Par exemple, le procureur de la République peut d'office ou sur demande des parties civiles rendre publiques certaines informations relatives à l'instruction en cours. Il s'agit de révéler des « éléments objectifs »[872] dans le but d'éviter la propagation de fausses informations ou pour mettre fin à un trouble à l'ordre public[873]. Par ailleurs, l'article 199 du code de procédure pénale prévoit la possibilité pour la personne concernée de demander à ce que l'audience relative à sa détention provisoire soit publique. Par extension, on peut considérer que les dispositions de l'article 11-1 qui prévoient la possibilité de transmettre des données issues du dossier d'instruction en cours, afin par exemple de faciliter l'indemnisation des victimes, constitue une limite au secret. Ces dispositions peuvent s'analyser comme marquant un affaiblissement au principe strict du secret et instaurent en pratique un semblant de « secret partagé »[874]. Enfin il faut admettre que l'instruction se veut de plus en plus contradictoire laissant aux parties davantage de droits au cours de la procédure[875].

---

l'enquête et de l'instruction : un policier n'est pas investi du droit de communiquer sur une enquête en cours, *RSC*, 2020, p. 682.

[869] Cass., civ. 2e, 21 janvier 1981, *pourvoi* n° 79-15686. Cette solution a été reprise par la chambre sociale dans un arrêt du 6 juillet 1994 (*pourvoi* n° 90-43640).

[870] Décret n°2005-790 du 12 juillet 2005 relatif aux règles de déontologie de la profession d'avocat, art. 5.

[871] *Ibid*.

[872] Art. 11 al. 3 du code de procédure pénale.

[873] *Ibid*.

[874] V. *infra* n°314 s.

[875] Toutes ces atténuations seront abordées dans la suite du raisonnement.

307. Le débat autour du maintien du secret de l'enquête et de l'instruction – Les débats se sont élevés sur une éventuelle refonte du secret de l'instruction. Dans un rapport du comité de réflexion sur la justice pénale déposé en septembre 2009 était envisagée la suppression du secret de l'instruction[876]. Alors que le rapport d'étape du 6 mars 2009 proposait un maintien du principe tout en dépénalisant sa violation, le rapport final suggère de supprimer le principe de secret de l'enquête et de l'instruction au nom du droit à l'information, rappelant également son caractère « fictif »[877]. Un rapport d'information de la commission des lois déposé fin 2019 rappelle le caractère essentiel du secret comme garant de l'efficacité des enquêtes. Néanmoins il observe que l'application du principe s'oppose au concept de transparence qui tend à se développer dans la société. Aussi, les auteurs constatent d'une part que malgré le principe de secret certaines données sont diffusées du fait de nombreuses exceptions existantes, et d'autre part que les sanctions visant la méconnaissance du principe ne sont que rarement appliquées. Face à ce constat, les auteurs suggèrent de maintenir le principe du secret de l'instruction mais de consacrer dans le code de procédure pénale un réel droit à l'information. La communication de données d'enquête ou d'instruction pourrait alors être justifiée par « l'impératif prépondérant d'intérêt public »[878]. Afin de trouver le juste équilibre entre le secret et le droit à l'information il est proposé de faciliter la communication par les acteurs de la chaine pénale sur les enquêtes en cours et d'encadrer davantage le rôle et l'intervention des journalistes dans les affaires. Le rapport suggère de repenser le partage d'informations en cours d'enquête entre les autorités judiciaires et les autorités administratives sur le modèle ce qui est déjà permis par l'article 11-2 du code de procédure pénale qui autorise les magistrats à transmettre à d'autres administrations des données sur des affaires en cours en organisant un secret partagé[879]. La communication publique sur les affaires en cours s'inscrit dans l'idée d'une justice transparente et ne peut se concevoir que si des garanties solides sont prévues préservant la bonne administration de la justice et aussi les données relatives aux individus visés dans ces affaires.

308. Instruction et données personnelles – Si l'on raisonne d'un point de vue des données personnelles et de la protection à laquelle les individus ont droit s'agissant de ces données, la communication de celles-ci de manière publique suppose de taire les données identifiantes ou

[876] Rapport du comité de réflexion sur la justice pénale déposé le 1er septembre 2010.
[877] Pré- Rapport du comité de réflexion sur la justice pénale déposé 6 mars 2009.
[878] Rapport d'information de l'assemblée nationale n°2540, déposé le 18 décembre 2019 relatif au secret de l'enquête et de l'instruction.
[879] *Ibid.*

celles qui par recoupement permettent l'identification des individus concernés sauf si cette communication est nécessaire. Quel que soit l'avenir du secret de l'instruction, dont la suppression ne cesse d'être abordée, il conviendrait de penser un système de protection qui se fonderait non sur la nature de la procédure mais sur celle des données concernées. Ainsi, sur le modèle de ce qui se fait dans certains pays anglo-saxon, il conviendrait d'apporter une protection particulière au cours de la phase d'instruction aux données identifiantes dans le but d'assurer le bon déroulement de celle-ci et de protéger la présomption d'innocence. Il apparait en effet plus opportun d'encadrer cette diffusion de garanties et de confier ce rôle aux autorités judiciaires en leur donnant davantage de prérogatives en la matière. Si l'on peut comprendre la nécessité de protéger les données d'enquête et d'instruction d'une diffusion publique massive, avec les risques que celle-ci peut engendrer, la communication aux parties peut quant à elle s'avérer nécessaire. L'équilibre est quoi qu'il en soit délicat à trouver entre les différents intérêts en présence.

2° La nécessaire communication des données du dossier aux parties

309. L'impact de la juridictionnalisation de l'enquête sur le secret – Le sujet de la communication des données de l'enquête amène à s'interroger sur la question de la juridictionnalisation de celle-ci[880]. Les nombreuses évolutions qu'a connu la procédure pénale et notamment la phase d'enquête au cours de la dernière décennie soulèvent utilement des interrogations en termes d'équilibre des droits au cours de cette phase d'enquête. S'agissant des données personnelles contenues dans le dossier de procédure, se pose plus encore la question de la communication du dossier dans une phase de la procédure qui se juridictionnalise mais qui, par principe, n'est pas contradictoire.

En effet, la phase juridictionnelle de la procédure et l'acquisition par les individus concernés d'un statut au sein de cette procédure confèrent des droits dont ils ne disposent pas lors de l'enquête. Cette juridictionnalisation s'est manifestée à de nombreux égards. Tout d'abord le procureur de la République a vu ses pouvoirs en matière d'enquête augmenter, notamment par l'admission du recours à la contrainte. Le procureur est désormais autorisé à faire réaliser grand nombres d'actes et dispose de prérogatives plus étendues et plus coercitives. Le développement de ces prérogatives a rendu nécessaire la mise en œuvre d'un contrôle des

[880] O. Décima, *La juridictionnalisation de l'enquête pénale*, coll. Actes et Etudes, Cujas, 2015.

actes par un juge du siège[881]. Aussi, le développement des procédés dérogatoires dont dispose le procureur de la République[882] conduisent certains auteurs à parler de « confusion saillante entre l'enquête de flagrance et le cadre d'investigation offert par l'instruction »[883]. A côté du développement de nouveaux procédés d'enquête, le procureur de la République a vu ses pouvoirs décisionnels en termes d'orientation des poursuites s'accroitre, lui permettant soit d'abandonner les poursuites, soit de saisir la juridiction de jugement soit encore de prononcer des alternatives aux poursuites.

S'agissant des procédures alternatives aux poursuites, on assiste à un développement exponentiel de celles-ci[884]. Ces procédures se sont développées et étoffées, laissant au procureur de la République un large choix quant aux suites données à l'affaire. Il faut notamment citer la mesure de composition pénale qui interroge quant au pouvoir juridictionnel attribué au Parquet[885]. Tout d'abord, parce que son prononcé est conditionné à la reconnaissance par la personne concernée des faits reprochés. Ensuite parce que les mesures qui peuvent être proposées peuvent être assimilées à des sanctions[886]. Enfin, un détail qui n'en n'est pas un, la mesure de composition pénale est inscrite au casier judiciaire. Tout cela amène à s'interroger sur les pouvoirs du procureur de la République à prononcer des « quasi-peines »[887] et de fait sur son statut de « quasi-juge »[888]. Les chiffres témoignent de la place importante de celles-ci dans la réponse pénale. Par exemple sur les chiffres de 2019, 606 225 affaires ont fait l'objet de poursuites et 528 692 mesures alternatives ont été décidées[889]. Finalement, ces mesures alternatives représentent quasiment la moitié des réponses apportées, témoignant de l'importance du rôle du procureur de la République en la matière.

---

[881] Voir sur la question, A. Gogorza, L'autorisation judiciaire pendant la phase policière, *RSC* 2017, 247. P. Le Monnier De Gouville, La juridictionnalisation de l'enquête pénale, *Les cahiers de la justice, Dalloz*, 2015, n°1, p. 136. Pour reprendre les termes de l'auteure, *« toute mesure de contrainte suppose un contrôle de l'autorité judiciaire »*, au regard de l'article 66 de la Constitution.

[882] Comme c'est le cas en matière de criminalité organisée en vertu de l'article 706-89 du code de procédure pénale.

[883] P. Le Monnier De Gouville, La juridictionnalisation de l'enquête pénale, *op. cit*., p. 131 à 139.

[884] F. Molins, *Action publique*, Répertoire de droit pénal et de procédure pénale, novembre 2017, actualisation avril 2020. A.S. Chavent-Leclère, Procédure pénale – Des évolutions en cours à la révolution attendue en procédure pénale, *Procédures*, 1er janvier 2015.

[885] Art. 41-2 et 3 du code de procédure pénale.

[886] Par exemple il peut s'agir d'une amende, de la remise de son permis de conduire, d'une interdiction d'émettre des chèques, d'une interdiction de quitter le territoire…

[887] J. C. Saint-Pau, Le ministère public concurrence-t-il le juge du siège ?, *Droit pénal*, n° 9, septembre 2007, et. 14.

[888] *Ibid.*

[889] Voir les chiffres clé de la justice sur le site du ministère de la justice, http://www.justice.gouv.fr/statistiques-10054/chiffres-cles-de-la-justice-10303/.

Si la Cour européenne des droits de l'homme a rappelé que le ministère public n'est pas une autorité judiciaire[890], des décisions et lois plus récentes semblent aller dans le sens d'une affirmation du phénomène de juridictionnalisation de l'enquête[891]. Aussi, le Conseil constitutionnel a clairement tranché en faveur du droit au recours juridictionnel effectif lors de la phase d'enquête. On peut notamment citer la décision du 21 mars 2014 relative à la saisie durant l'enquête de biens ayant servi à commettre l'infraction. Le Conseil constitutionnel a retenu que la mesure de saisie n'étant ni contradictoire ni contestable, elle violait la Constitution[892]. De manière plus générale, le Conseil constitutionnel a jugé que la faculté pour le procureur de la République d'ordonner la destruction, en cours d'enquête, d'objets saisis ayant une nature dangereuse, sans que les propriétaires ne disposent d'un quelconque recours, était contraire à l'article 16 de la Déclaration de 1789[893].

310. Impact de la juridictionnalisation en termes de données personnelles – Les constats précédents amènent une partie de la doctrine à parler de « partie à l'enquête ». Finalement, dans ce nouveau contexte, on peut s'interroger sur la place de l'individu visé par une enquête tant sur son droit de s'opposer à la réalisation de certains actes que sur son droit à se faire communiquer les pièces du dossier. La première question intéresse moins le sujet des données à caractère personnel bien qu'on puisse admettre que la diminution de la place du consentement dans la réalisation des actes de procédure lors d'une enquête de flagrance ou préliminaire a *de facto* rendu les données relatives à la personne plus accessibles aux enquêteurs[894]. C'est davantage la question de la communication des pièces du dossier d'enquête qui intéresse le sujet. Le développement de nouvelles prérogatives dès le stade de

[890] Cour E.D.H., 5e sect., 10 juillet 2008, *Medvedyev et a. c/ France*, n°3394/03.
[891] C'est le cas des lois adoptées en matière de lutte contre le terrorisme qui tendent de plus en plus au développement de procédés dérogatoires accentuant les pouvoirs d'enquête. Voir par exemple au sujet de loi du 3 juin 2016 de lutte contre le terrorisme, O. Décima, Terreur et métamorphose, *Recueil Dalloz*, 2016, p. 1826.
[892] Cons. const., 21 mars 2014, n°2014-375 QPC.
On peut également citer la décision du 2 décembre 2011, n°2011-203 QPC. Se prononçant sur la procédure d'aliénation des biens saisis par les douanes, le Conseil constitutionnel a considéré que la mesure n'étant ni contradictoire ni suspensive elle était contraire à la Constitution. X. Delpech, Inconstitutionnalité de la vente des biens saisis par l'administration douanière, *Dalloz actualité*, 6 décembre 2011.
[893] Cons. const., 11 avril 2014, n°2014-390 QPC. A. Botton, Le droit à un recours juridictionnel effectif dans le cadre de l'enquête pénale, *Dalloz, Constitutions*, 2014, p. 471. L'auteur souligne utilement, qu'il s'agit de la première décision du Conseil constitutionnel dans laquelle ce dernier vise directement une disposition de code de procédure pénale et la sanctionne au vu de l'article 16 de la déclaration de 1789 marquant de ce fait la réelle volonté de reconnaitre un droit au recours juridictionnel dès la phase d'enquête.
[894] L'article 76 du code de procédure pénale dispose depuis la loi du 9 mars 2004 que les perquisitions domiciliaires peuvent « si les nécessités de l'enquête l'exigent » être effectuées sans le consentement de la personne. On peut également citer la décision QPC du Conseil constitutionnel du 4 avril 2014 dans laquelle le Conseil constitutionnel a considéré que l'absence de voie de recours pour les personnes concernées par une perquisition réalisée dans le cadre d'une enquête viole la Constitution. Cons. const. 2014-387 QPC.

l'enquête appelle au renforcement du contrôle juridictionnel de ces actes et soulève la question pour les individus concernés de l'accès aux données de l'enquête. Des dispositions récentes tendent à faire entrer le contradictoire dans la phase d'enquête mais force est de constater que cela reste limité.

311. La communication limitée des pièces dans le cadre d'un placement en garde à vue – L'article 63-4-1 du code de procédure pénale prévoit la possibilité pour l'avocat d'une personne placée en garde à vue de consulter le procès-verbal notifiant la mesure, le certificat médical ainsi que les procès-verbaux d'audition. L'avocat a accès aux pièces sans pouvoir pour autant en obtenir de copie. Ces dispositions sont la conséquence d'une évolution des textes en faveur d'un droit à l'accès au dossier d'enquête par les « parties ». La directive européenne du 22 mai 2012 relative au droit à l'information dans les procédures pénales prévoit pour les personnes détenues l'accès aux documents utiles à la contestation de la légalité de la mesure[895]. Aussi, toute personne suspecte ou poursuivie doit avoir accès à toutes les données probatoires au nom du principe d'équité et des droits de la défense[896]. La contestation de la légalité d'une mesure de détention y donne accès à tout moment. *A contrario,* les droits de la défense justifient un accès aux données « en temps utile »[897]. Néanmoins ce droit d'accès est plus retreint en matière de garde à vue que lors de la phase juridictionnelle d'instruction. En effet, l'avocat ne peut alors consulter que certaines pièces du dossier (le procès-verbal de notification de placement en garde à vue, le certificat médical ainsi que les procès-verbaux d'audition). La Cour européenne des droits de l'homme semble d'ailleurs aller dans ce sens en considérant qu'il peut être nécessaire de garder certaines données d'enquête secrètes afin d'éviter par exemple l'altération de preuves[898]. Si dans une décision plus récente la Cour européenne des droits de l'homme semble affirmer que les restrictions dans l'accès au dossier peuvent porter atteinte aux droits de la défense[899], dans sa décision *A.T. c/ Luxembourg* du 9 avril 2015, elle affirme clairement que l'article 6 de la convention ne trouve pas à s'appliquer à la phase pré-juridictionnelle. La cour européenne considère que *«l'article 6 de la Convention ne saurait être interprété comme garantissant un accès illimité au dossier pénal dès avant le premier interrogatoire par le juge d'instruction,*

[895] Directive, 2012/13/UE du parlement européen et du conseil, du 22 mai 2012 relative au droit à l'information dans le cadre des procédures pénales. Art. 7.
[896] *Ibid.*
[897] *Ibid.*
[898] Cour E.D.H., 9 mars 2006, *Svipsta c/ Lettonie*, 66820/01, §137.
[899] Cour E.D.H., 20 septembre 2011, Sapan c/ Turquie, 177252/09, §21. F. Desprez, Garde à vue : consultation des pièces de procédure par l'avocat, *Recueil Dalloz,* 2013, p. 2760.

lorsque les autorités nationales disposent de raisons relatives à la protection des intérêts de la justice suffisantes pour ne pas mettre en échec l'efficacité des investigations »[900]. La chambre criminelle de la Cour de cassation a statué en ce sens, estimant que l'accès limité au dossier au stade de l'enquête ne porte pas atteinte aux droits de la défense[901]. Le droit à un accès illimité aux données de l'enquête est souvent invoqué au nom des droits de la défense prônant ainsi la reconnaissance d'un réel statut de « partie » dès le stade de l'enquête[902]. Toutefois, cet accès illimité pourrait, sans un contrôle juridictionnel strict, porter atteinte au bon déroulement de l'enquête. La reconnaissance de l'enquête comme phase juridictionnelle de la procédure aurait pour conséquence d'attribuer aux individus visés par une enquête les mêmes droits que dans la phase juridictionnelle et de les soumettre aux mêmes interdictions. Pour l'heure, si les parties à l'instruction ne sont pas soumises au secret de l'instruction, les dispositions de l'article 114-1 du code de procédure pénale pose l'interdiction de révéler aux tiers les informations de la procédure sous peine de sanction.

312. La communication du dossier relatif à une enquête longue – Si au cours de l'enquête le principe du secret ne permet pas l'accès aux pièces du dossier, depuis l'entrée en vigueur de la loi du 3 juin 2016[903], toute personne contre laquelle existent des raisons plausibles de soupçonner qu'elle a commis ou tente de commettre une infraction punie d'une peine privative de liberté, faisant l'objet d'une audition ou d'un placement en garde à vue peut, un an après l'exécution du premier acte, demander à consulter le dossier de procédure. L'article 77-2 du code de procédure pénale fixe les modalités de consultation. Lorsque la personne mise en cause fait une demande de consultation du dossier, le procureur de la République informe la victime ayant déposé plainte de son droit à consulter le dossier dans les mêmes conditions. De manière générale la question de l'accès au dossier d'enquête soulève des divergences d'opinions. Certains voient dans le secret une atteinte aux droits de la défense et d'autres considèrent qu'une trop grande communication peut nuire au bon déroulement de la procédure[904]. Si le contradictoire semble s'immiscer dans la phase d'enquête, ce phénomène

[900] Cour E.D.H., 9 avril 2015, *A.T. c/ Luxembourg*, n°30460/13, cons. 80 à 83. La Cour européenne des droits de l'homme précise à cette occasion que sa position affirmée dans cet arrêt ne peut être remise en cause par l'arrêt précité Sapan c/ Turquie mettant ainsi un terme à certaines interrogations nées de cette affaire.
[901] Cass., crim., 12 septembre 2012, *pourvoi* n°11-88.111.
[902] Sur la notion, voir Y. Capdepon, *Essai d'une théorie générale des droits de la défense*, préf. J.C. Saint Pau, Dalloz, 2013.
[903] Loi 2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale.
[904] J. Beaumes, *Rapport sur la procédure pénale*, juillet 2014, doc. fr.. L'auteur avance divers arguments. Tout d'abord d'un point de vue strictement matériel, il soulève les difficultés que peuvent engendrer la communication des dossiers de procédure notamment lorsque ces dernières sont longues et comportent beaucoup

reste limité. La loi du 3 juin 2016 marque les prémices d'une forme de contradictoire dans l'enquête. En effet, un individu faisant l'objet d'une enquête n'a pas accès à toutes les données de celle-ci et ne sait, de fait, pas l'étendue de ce qui lui est potentiellement reproché. Cela s'explique par la nécessité de ne pas nuire à l'enquête. De plus, les différents procès-verbaux dressés comportent nécessairement des données relatives à grand nombre d'individus identifiés constituant de fait des données à caractère personnel. Elles peuvent de surcroit constituer des données sensibles au sens de la loi informatique et libertés notamment lorsque le procès verbal fait état de données d'ordre médical. Aussi, les procès-verbaux peuvent relater des données judiciaires. Au-delà des considérations d'ordre pratique liées à la bonne conduite de l'enquête et aux nécessités d'assurer la protection des preuves contre d'éventuelles altérations, le secret de l'enquête protège contre les risques d'atteintes liées à la diffusion de données personnelles que contiennent nécessairement les dossiers de procédure.

313. La communication du dossier en cours d'instruction – Au cours de la phase d'instruction, qui est une phase juridictionnelle de la procédure, les parties disposent d'un droit à la communication du dossier pénal. Ce droit est encadré par les textes. Ainsi, au cours de l'instruction et avant tout interrogatoire ou toute confrontation, le dossier peut être mis à la disposition des parties par le biais de leur avocat dans les conditions prévues à l'article 114 du code de procédure pénale. Selon une jurisprudence constante, la communication vise le dossier dans son intégralité dans l'état dans lequel il se trouve au moment où il est transmis[905]. Sous l'influence de la jurisprudence de la Cour européenne des droits de l'homme[906], le législateur a atténué les dispositions applicables en la matière en adoptant la loi du 30 décembre 1996 permettant aux parties d'obtenir une copie des pièces du dossier d'instruction[907]. Ces dernières devaient être informées de l'interdiction de divulguer les données contenues dans le dossier[908]. Désormais, les dispositions de l'article 114 du code de

---

de procès-verbaux. Cela induit de facto de laisser un temps nécessaire à l'avocat à la lecture du dossier avant de poursuivre la procédure. L'auteur fait également référence aux enjeux en termes d'efficacité de l'enquête. En fonction de la nature de celle-ci l'impact en termes d'efficacité peut différer et s'avérer plus négatif s'agissant d'enquêtes « lourdes ».

[905] De jurisprudence constante depuis, Cass., crim., 9 février 1982, bull. 47, *JCP* 83 II, 1973.

[906] Cour E.D.H., 18 mars 1997, *Foucher c/ France*, n°22209-93. En l'espèce, le requérant avait fait le choix de ne pas être représenté par un avocat et invoquait l'atteinte aux droits de la défense liée au refus d'accès au dossier qui lui avait été opposé. Néanmoins il convient de rappeler que dans l'arrêt *Kremzow c/ Autriche* du 21 septembre 1993 (12350/86), la Cour européenne des droits de l'homme a affirmé que le fait de ne laisser qu'un accès indirect au dossier c'est-à-dire par le biais de l'avocat à la partie n'est pas incompatible avec les droits de la défense.

[907] Loi n°96-1235 du 30 décembre 1996 relative à la détention provisoire et aux perquisitions de nuit en matière de terrorisme.

[908] Art. 114-1 du code de procédure pénale.

procédure pénale prévoient que les parties qui n'ont pas d'avocat peuvent se faire délivrer directement copie des pièces du dossier. La communication du dossier d'instruction se trouve alors facilitée en ce qui concerne les parties. Cette communication des données de procédure est également nécessaire entre les différentes autorités intervenant au cours de la procédure, renvoyant à l'idée d'un secret partagé.

§2. Le secret partagé applicable aux données des procédures judiciaires

314. Notion de secret partagé – En l'état actuel du droit le terme de secret « partagé » n'a pas été, à proprement parler, consacré s'agissant du secret de l'enquête ou de l'instruction. En effet, cette notion n'est en réalité pas définie par la loi et tend à renvoyer pour l'heure au partage d'informations entre professions médicales ou sociales[909]. Néanmoins, on ne peut nier l'existence d'un partage de données couvertes par le secret dans les procédures pénales d'enquête et d'instruction. L'idée d'une consécration du secret partagé applicable au domaine de la justice avait été suggérée lors de la réforme du code pénal, puis abandonnée[910]. La communication du dossier pénal entre les différents intervenants dans la procédure relève plutôt du « partage de données à caractère secret »[911], nécessaire au bon déroulement de la procédure. En ce sens certains auteurs renvoient au « secret procédural »[912] qui peut de fait être partagé entre tous les intervenants de « l'équipe procédurale »[913] qui regroupe tous les intervenants de la procédure et auxiliaires du juge d'instruction. Ce secret procédural tend à s'appliquer à tous les « confidents nécessaires »[914] du magistrat sur le modèle du secret

[909] En effet, s'il est souvent fait référence à la notion de « secret partagé », cette dernière n'apparait pas strictement dans les textes. Elle est toutefois souvent rattachée au secret médical et à la loi du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé (Loi n°2002-303). Cette loi a inséré dans le code de la santé publique les dispositions relatives à la possibilité pour un médecin d'échanger, sous certaines conditions, des informations médicales avec un confrère (article 1110-4). Des dispositions similaires ont ensuite été insérées dans le code de l'action sociale et des familles en matière de protection de l'enfance permettant de la même manière l'échange d'informations entre professionnel du secteur (article 226-2-2, loi n°2007-293 du 5 mars 2007 réformant la protection de l'enfance).

[910] Circulaire du 14 mai 1993 commentant les dispositions de la partie législative du nouveau code pénal. Lors de la réforme du code pénal qui a conduit à la réécriture de l'article 226-13 du code pénal, le Gouvernement avait proposé d'inscrire le principe de secret partagé dans le nouveau code. Cette idée a été rejetée notamment du fait du flou entourant la notion.

[911] Voir, M. Medjkane, Le partage des informations à caractère secret, *AJ Pénal*, 2017, p. 371. L'auteur renvoie à la notion de partage d'informations à caractère secret en matière de lutte contre le terrorisme.

[912] C. Ribeyre, *La communication du dossier pénal*, Presses universitaires d'Aix-Marseille, 2007, p.99 et s. Du même auteur, La communication du dossier aux parties privées, JCP G, 2006, chron. 152.

[913] C. Ribeyre, *La communication du dossier pénal*, *op. cit.*

[914] *Ibid.*

partagé appliqué en matière médico-sociale[915]. Ainsi, les données de procédure font l'objet de partages que ce soit de par le biais du partage de dossiers entre magistrats (A.) ou avec l'administration (B.).

A. Le partage de dossiers entre magistrats

315. La nécessaire communication au sein de la juridiction – L'application du principe du secret de l'enquête et de l'instruction peut soulever des interrogations liées à l'échange d'informations entre magistrats. Par l'exercice de leurs prérogatives ou du fait de dispositions particulières, les magistrats peuvent être amenés à se communiquer, entre eux, les dossiers de procédures. Par exemple, le procureur de la République peut se faire communiquer tout dossier en cours d'instruction au sein de sa juridiction[916]. Il dispose ainsi d'un droit de regard sur les dossiers en cours au sein de sa juridiction et peut accéder aux données du dossier qui lui semblent utiles pour requérir des actes ou mesures de sûreté. AU demeurant, en vertu des dispositions de l'article L.122-4 du code de l'organisation judiciaire, le ministère public est indivisible ce qui signifie qu'un magistrat du Parquet peut exercer les fonctions du ministère public au sein de sa juridiction. Ce principe se retrouve dans différents articles du code de procédure pénale. Ainsi, le procureur ou ses substituts peuvent représenter le ministère public auprès du tribunal judiciaire, de la Cour d'assises, du tribunal de police ou de la Cour d'appel[917]. Le principe d'indivisibilité signifie que le ministère public peut être représenté « dans la même cause »[918] par des magistrats différents, qui de fait ont connaissance du dossier. Enfin, en cas d'urgence le juge instructeur peut être suppléé par un autre juge d'instruction du même tribunal chargé de prendre des actes isolés[919]. Le magistrat suppléant n'est pas désigné par ordonnance du président et le caractère urgent n'a pas à être démontré[920]. La chambre criminelle de la Cour de cassation a précisé que l'empêchement du juge n'avait pas non plus à être démontré[921]. Sans que ne soit violé le secret, la communication des données du dossier peut s'avérer nécessaire au delà de la juridiction mais celle-ci reste très encadrée.

[915] *Ibid.*
[916] Art. 82 al 2 du code de procédure pénale.
[917] Art. 39 et 34 du code de procédure pénale.
[918] Cass., crim., 2 décembre 1959, bull. 524.
[919] Art. 84 al 4 du code de procédure pénale. Voir, L. Belfanti, *Juge d'instruction*, Répertoire de droit pénal et de procédure pénale, *op. cit.*, 318.
[920] Cass., crim., 24 janvier 1984.
[921] Cass., crim., 6 octobre 2015, *pourvoi* n°15-81.665. Voir, C. Guéry, *Instruction pénale*, Répertoire de droit pénal et de procédure pénale, juin 2018 actualisation novembre 2020.

B. Le partage de dossiers judiciaires avec l'administration

316. Partage prévu par les dispositions de l'article 11-1 du code de procédure pénale – L'article 11-1 du code de procédure pénale dispose que « Sur autorisation du procureur de la République ou du juge d'instruction selon les cas, peuvent être communiqués à des autorités ou organismes habilités à cette fin par arrêté du ministre de la justice, pris le cas échéant après avis du ou des ministres intéressés, des éléments des procédures judiciaires en cours permettant de réaliser des recherches ou enquêtes scientifiques ou techniques, destinées notamment à prévenir la commission d'accidents, ou de faciliter l'indemnisation des victimes ou la prise en charge de la réparation de leur préjudice. Les agents de ces autorités ou organismes sont alors tenus au secret professionnel en ce qui concerne ces informations ». Cela marque une première atténuation au principe de secret de l'enquête et de l'instruction.

317. Le partage de données avec l'administration fiscale – L'article L101 du livre des procédures fiscales prévoit une obligation d'information à l'administration fiscale. Cette dernière peut obtenir du procureur de la République qu'il lui communique toute information sur une enquête en cours susceptible de révéler une fraude fiscale[922]. Il s'agit donc d'une entraide entre autorités judiciaires et administration fiscale. Toutefois ce mécanisme de communication a soulevé des interrogations. L'article L101 du livre des procédures fiscales dispose que « l'autorité judiciaire doit communiquer à l'administration des finances toute indication qu'elle peut recueillir, de nature à faire présumer une fraude… ». Ces dispositions laissent sous entendre une obligation incombant à l'autorité judicaire. Cette obligation vaut pour les affaires jugées ou en cours d'enquête ou d'instruction et apparait comme le corollaire de l'article 40 du code de procédure pénale qui impose aux agents de la fonction publique de porter sans délai à la connaissance du procureur de la République des faits délictueux dont ils ont connaissance. Il s'agit donc d'une obligation spontanée qui n'empêche pas l'administration de demander la transmission des pièces[923]. L'article L82C du code des procédures fiscales précise qu'à l'occasion de toute instance civile ou criminelle, le procureur de la République peut communiquer les pièces du dossier à l'administration des finances. Ces dispositions visent toutes les pièces du dossier pénal sans restriction.

[922] CE, 22 novembre 1978, n°06557.
[923] CE, 3 décembre 1990, n°103101, SA Antipolia.

318. Les conséquences de la nullité des pièces pénales – La question a été soulevée des conséquences d'une nullité des pièces pénales sur celles transmises au titre du droit de communication. Le Conseil d'Etat dans un arrêt rendu le 6 décembre 1995[924] a précisé que si les pièces pénales étaient déclarées nulles postérieurement à leur transmission aux autorités de finance, cela n'avait pas d'incidence sur la légalité des pièces devant l'administration fiscale. De la même manière, dans un arrêt du 24 novembre 1997[925], le Conseil d'Etat a conclu en la recevabilité des pièces obtenues par usage du droit de communication. Saisie dans cette affaire, la Cour européenne des droits de l'homme a considéré que la saisie domiciliaire ayant permis le recueil des pièces avait porté une atteinte excessive au droit au respect de la vie privée, entrainant la nullité des pièces[926]. Toutefois, le Conseil d'Etat, dans sa décision du 24 novembre 1997, a considéré que l'arrêt de la Cour européenne des droits de l'homme « rendu après que l'administration fiscale eut obtenu communication d'une partie des pièces saisies […], n'a pas eu pour effet de la priver du droit de se prévaloir des informations contenues dans ces dernières, à titre d'éléments de preuve ». L'arrêt de la Cour européenne des droits de l'homme étant intervenu après que l'administration ait fait jouer son droit de communication, elle n'entachait pas la procédure fiscale fondée sur les pièces litigieuses. La chambre criminelle de la Cour de cassation a repris ce raisonnement dans un arrêt du 19 janvier 2000 rappelant que *« la nullité éventuelle de pièces ou d'actes établis dans une procédure distincte de droit commun, régulièrement communiqués à l'administration des Impôts en application de l'article L. 101 du Livre des procédures fiscales, et versés dans la procédure ultérieurement engagée du chef de fraude fiscale, ne peut être invoquée dans le cadre de cette dernière procédure »*[927].

S'agissant des données à caractère personnel contenues dans le dossier pénal, ce mécanisme permet une communication de l'entier dossier à l'administration sans accorder une protection particulière aux données personnelles sensibles ou judiciaires des individus, et ce, quand bien même la procédure pénale serait entachée de nullité. La garantie tient dans le secret professionnel auquel sont tenus les agents de l'administration fiscale dans l'exercice de leurs fonctions et qui « s'étend à toutes les informations recueillies »[928]. Au-delà des limites posées

[924] CE., 6 décembre 1995, n°126826.
[925] CE., 24 novembre 1997, n°171929. Voir, Régularité du droit de communication exercé par l'administration fiscale et influence d'un arrêt rendu par la Cour européenne des droits de l'homme sur la valeur probante des documents saisis, *Recueil Dalloz*, 1996, p. 159.
[926] Cour. E.D.H., 25 février 1993, *Miailhe c/ France*, requête n°12661/87. Voir, G. Tixier, A.G. Hamonic-Gaux, Portée du droit de communication de l'administration fiscale et compatibilité des arrêts de la Cour européenne des droits de l'homme et des arrêts du Conseil d'Etat, *Dalloz*, 1998, p. 159.
[927] Cass., crim., 19 janvier 2000, *pourvoi* n°98-86728.
[928] Art. L103 du livre des procédures fiscales.

au principe de secret de l'enquête et de l'instruction, la communication des pièces du dossier peut s'avérer nécessaire pour les parties.
Si le secret de l'enquête et de l'instruction connait des limites et exceptions, sa violation constitue une infraction à laquelle il convient de s'intéresser plus en détail.

§3. La communication illégale de données issues de procédures d'enquête et d'instruction

319. Les délits de violation du secret de l'enquête et de l'instruction peu sanctionnés – La question des sanctions liées à la méconnaissance du principe de secret de l'enquête et de l'instruction fait débat. En effet, si les textes renvoient en la matière aux dispositions des articles 226-13 et 226-14 du code pénal relatifs à la violation du secret professionnel[929], dans les faits ces dispositions sont peu utilisées s'agissant du secret de l'enquête et de l'instruction. Si le principe du secret de l'enquête et de l'instruction est présenté comme principe fondateur de la procédure pénale force est de constater que sa méconnaissance reste peu sanctionnée. Pourtant, au-delà des articles 226-13 et 226-14 du code pénal d'autres dispositions condamnent la violation du secret. Par exemple, l'article 114-1 du code de procédure pénale pose l'interdiction pour les parties de diffuser une pièce du dossier d'instruction avant clôture de celle-ci. Dans le rapport remis en décembre 2019, la Commission des lois a mis en évidence les rares condamnations prononcées sur le fondement d'une violation du secret de l'enquête et de l'instruction[930]. Les dispositions de l'article 11 du code de procédure pénale ne visent que les personnes qui « concourent » à la procédure étant entendu que les avocats ou les parties civiles ne sont pas visés. Ainsi, un grand nombre de personnes disposant d'informations relatives à l'enquête ou l'instruction en cours ne sont pas soumises au principe du secret. Les auteurs visent également les atténuations au principe qui permettent notamment au procureur de la République de communiquer sur un dossier en cours. Le rapport de la Commission des lois met en exergue le fait que des sanctions disciplinaires sont plus souvent prononcées à l'égard notamment des agents de police sur le fondement de la violation de leur obligation de discrétion[931] que sur celui de violation du secret de l'enquête et de l'instruction.

[929] Art. 11-1 du code de procédure pénale.
[930] Rapport d'information de la Commission des lois n°2540 déposé le 18 décembre 2019 relatif au secret de l'enquête et de l'instruction.
[931] Art. R. 434-8 du code de la sécurité intérieure.
A titre d'exemple, le rapport informe que s'agissant du délit d'entrave à l'exercice de la justice par révélations volontaires d'informations (art. 434-7-2 du code pénal), ce dernier a donné lieu à deux condamnations en 2017.

Finalement, le secret de l'enquête et de l'instruction semble affaibli par la liberté d'expression, le droit à l'information et le secret des sources et l'équilibre semble ainsi difficile à trouver.

320. Les effets de la violation du secret sur la procédure – La Cour de cassation a eu l'occasion de revenir sur la question de l'effet d'une violation du secret de l'enquête et de l'instruction sur la procédure en cours[932]. Dans un arrêt du 10 janvier 2017, la chambre criminelle a rappelé que si la violation est postérieure à l'acte, celle-ci n'affecte pas sa validité[933]. On admet aisément que l'acte ayant été réalisé régulièrement, le délit commis après ne l'affecte pas directement. Si la violation du secret est concomitante à la réalisation de l'acte la Cour de cassation considère dans l'arrêt du 10 janvier 2017 que cette violation porte nécessairement atteinte aux droits de la défense. En ce sens, la Cour de cassation adopte une analyse nouvelle. Jusqu'alors, cette dernière considérait que l'atteinte aux droits de la défense devait être caractérisée pour que la violation du secret entache l'acte de procédure[934].

321. Une protection assurée s'agissant de la révélation d'une donnée secrète par une personne non dépositaire – Sans viser nécessairement directement la violation du secret de l'enquête et de l'instruction, les données de la procédure sont protégées par le biais d'autres incriminations. La question se pose notamment s'agissant de la diffusion par la presse de données issues de procédure[935]. Si elle défend un droit à l'information au nom de la liberté d'expression, la Cour européenne des droits de l'homme a parfois condamné les faits commis par des journalistes pour l'atteinte portée à la présomption d'innocence ou atteinte au bon déroulement de l'enquête. Dans un arrêt du 24 novembre 2005, *Tourancheau et July c/ France*,[936], la Cour européenne des droits de l'homme a eu à se prononcer à la suite de la condamnation par les juridictions internes de journalistes sur le fondement de l'article 38 de la loi du 29 juillet 1881 qui pose l'interdiction de publier des actes de procédure avant qu'ils n'aient été rendus publics. Il était reproché à ces derniers d'avoir méconnu la loi en publiant

---

Une seule condamnation a été prononcée pour délit d'entrave à la justice par pressions exercées en vue d'influencer les témoins ou le juge (art. 434-16 du code pénal), enfin, la violation du secret et le recel de violation du secret de l'instruction visée à l'article 11 ont donné lieu à cinq condamnations cette même année.

[932] F. Cordier, Violation du secret de l'enquête ou de l'instruction et validité de l'acte accompli : la rigueur accrue de la chambre criminelle, *RSC*, 2017, p. 334.

[933] Cass., crim., 10 janvier 2017, *pourvoi* n°16-84.740. Dans cet arrêt, du 10 janvier 2017, il s'agissant d'une perquisition à laquelle avait assisté un journaliste et qu'il avait partiellement filmée.

[934] Cass., crim., 25 janvier 1996, *Bull. crim*..n° 53.

[935] Voir, E. Derieux, *Droit des médias*, LGDJ, 8e éd., 2018, 991 p.

[936] Cour E.D.H., 1ère section, 24 novembre 2005, n°53886/00, *Tourancheau et July c/ France*.

des pièces d'une procédure en cours. La Cour a considéré que l'atteinte faite à la liberté d'expression était justifiée par un but légitime visant notamment à assurer la protection de la présomption d'innocence[937]. Ainsi, la Cour européenne des droits de l'homme admet une atteinte à la liberté d'expression et limite la possibilité de diffuser des données issues de la procédure en cours dans le but de protéger les individus concernés et plus précisément leur droit à être présumés innocents. En ce sens, ces dispositions et l'interprétation faite par la Cour européenne des droits de l'homme constituent une protection des données à caractère personnel de la procédure. Par ailleurs, la jurisprudence de la Cour européenne admet le concept de « débat d'intérêt général »[938] justifiant une ingérence dans le droit au respect de la vie privée.

Dans certains litiges, une sanction peut être prononcée sur le fondement de la révélation d'une donnée secrète sans pour autant que l'individu n'ait violé le secret de l'enquête n'y étant pas soumis. Par exemple, dans l'arrêt du 29 mars 2016, *Bédat c/ Suisse*, la Cour européenne des droits de l'homme fait primer le secret de l'instruction sur la liberté d'expression. En effet, la Cour européenne va considérer que bien que relevant du débat d'intérêt général, les révélations faites par un journaliste sur une instruction en cours n'étaient pas pertinentes. Le journaliste n'est pas en droit suisse soumis au principe de secret de l'enquête. Sa condamnation repose sur la révélation sans autorisation d'actes d'instruction en cours[939]. La Cour européenne des droits de l'homme a considéré que cette condamnation ne portait pas une atteinte excessive à la liberté d'expression distinguant les informations pertinentes de la recherche de « sensationnel »[940]. La liberté de la presse au nom de la liberté d'expression et d'un droit à informer trouve donc des limites dans le but même de l'information communiquée et dans l'atteinte potentielle à la présomption d'innocence. S'il peut être admis que les journalistes communiquent en cours de procédure sur une affaire notamment lorsque celle-ci est très médiatisée et intéresse l'opinion publique, cette communication ne doit pas porter atteinte au bon déroulement de la justice. Il faut finalement distinguer les informations et données qui peuvent légitimement être communiquées au public et celles dont ils n'ont pas à avoir connaissance, sous peine de nuire au bon déroulement de l'enquête en cours et voir par

[937] Il est toutefois intéressant de noter que sur les sept juges, trois ont émis une opinion dissidente estimant qu'il ne fallait pas nécessairement brimer la liberté d'expression.

[938] Cour E.D.H., Gde. ch., 7 février 2012, *Von Hannover II c/ Allemagne* et Cour E.D.H., 10 novembre 2015, *Couderc et Hachette Filipacchi associés c/ France*. Dans ces deux arrêt, la Cour E.D.H. a considéré que le fait pour la presse de divulguer des photographies ou des informations relatives à la vie privée d'individus connus pouvait relever d'un débat d'intérêt public justifiant une ingérence dans le droit au respect de la vie privée n'entrainant de ce fait pas une atteinte excessive.

[939] Art. 293 du code pénal Suisse.

[940] Cour E.D.H., Gde. ch., 29 mars 2016, n° 56925/08, *Bédat c/ Suisse*.

exemple se déchainer le « tribunal populaire et/ou numérique » qui émet un « jugement » sans être juge et sans avoir les éléments nécessaires pour le faire. La jurisprudence interne semble aller dans ce sens en confirmant par exemple le bien fondé d'une décision condamnant des journalistes ayant publié un portrait robot en cours d'enquête[941] ou un rapport d'expertise relatif au mis en cause, sur le fondement de l'article 38 de la loi du 29 juillet 1881[942]. Cela soulève la question plus générale de la révélation dans la presse de l'identité des suspects.

Il ressort des dispositions de l'article 11 du code de procédure pénale que des dérogations à l'interdiction de communiquer peuvent être prévues par la loi. En ce sens, la presse peut être autorisée par le procureur de la République ou le juge d'instruction à diffuser des données protégées par le secret de l'instruction. Cette dérogation permet le recours à divers procédés visant à faire avancer l'enquête, tels que la diffusion de portrait-robot ou les appels à témoins. Toutefois, cette diffusion doit être autorisée et diligentée par un magistrat. Cela fait écho à la décision récente de la Cour européenne des droits de l'homme qui a validé la condamnation d'un journaliste pour recel de violation du secret de l'instruction. Ce dernier a diffusé de sa propre initiative le portrait-robot d'un suspect. La Cour de cassation a considéré que le portrait-robot avait nécessairement été transmis en violation du secret de l'instruction, ce que le journaliste ne pouvait ignorer[943]. La Cour européenne a considéré que l'ingérence dans la liberté de la presse était justifiée, nécessaire et légitime et n'y portait pas une atteinte excessive[944].

322. L'incrimination de recel appliqué à la violation du secret de l'instruction – Les journalistes ne sont donc pas tenus au secret de l'instruction et aux dispositions de l'article 11 du code de procédure pénale. La loi du 29 juillet 1881 prohibe cependant la diffusion d'éléments relatifs à des procédures en cours tant que ceux-ci n'ont pas été rendus publics en audience. Néanmoins, les articles 2 et 2 bis de la loi du 29 juillet 1881 relatifs au secret des sources, n'imposent pas au journaliste de révéler la provenance des données dont il a eu connaissance ni de fournir l'identité de l'individu qui en est à l'origine. Toutefois, le fait de révéler des informations relatives à une procédure en cours peut constituer une infraction de violation du secret et le journaliste utilisant cette donnée peut être poursuivi pour recel de violation. La consécration du délit de recel de violation du secret de l'instruction dans la

[941] Cass., crim., 9 juin 2015, *pourvoi* n°14-80.713.
[942] Cass., crim., 28 janvier 2014, *pourvoi* n°12-88.430. L'article 38 de la loi du 29 juillet 1881 dispose qu' « Il est interdit de publier les actes d'accusation et tous autres actes de procédure criminelle ou correctionnelle avant qu'ils aient été lus en audience publique et ce, sous peine d'une amende de 3 750 euros ».
[943] Cass., crim., 9 juin 2015, *pourvoi* n° 14-80.713.
[944] Cour E.D.H., 17 décembre 2020, req. n° 61470/15, *Sellami c/ France*.

jurisprudence démontre la volonté d'assurer une protection supplémentaire des données de l'instruction couvertes par le secret. L'article 321-1 du code pénal définit le recel comme « le fait de dissimuler, de détenir ou de transmettre une chose, ou de faire office d'intermédiaire afin de la transmettre, en sachant que cette chose provient d'un crime ou d'un délit. Constitue également un recel le fait, en connaissance de cause, de bénéficier, par tous moyens, du produit d'un crime ou d'un délit ». La chambre criminelle de la Cour de cassation est venue dès 1995 préciser l'application de ces dispositions s'agissant du recel d'informations issues d'une instruction en cours. Parmi les applications qui ont pu être faites de l'infraction de recel, il s'agit ici d'une « dématérialisation »[945] du délit. Cette volonté de protection se retrouve plus encore dans l'application faite du texte. Si en matière de recel d'informations couvertes par un secret il convient d'identifier le dépositaire qui a violé le secret constituant ainsi l'infraction préalable[946], en matière de recel du secret de l'instruction cette preuve n'est pas nécessaire[947].

Cette application du texte démontre la volonté de renforcer la protection du secret lors de la phase d'enquête et d'instruction. Bien que le soit affirmé strictement s'agissant de l'enquête et de l'instruction, la confidentialité occupe une place plus relative dans la phase d jugement.

Section 2 : Une confidentialité relative lors de la phase de jugement

323. Relativité attachée à une protection directe ou indirecte – La phase de jugement dans une procédure est en principe publique et soumise au contradictoire. Cette diffusion des données de procédure soulève la question de la protection des données de procédure. Cependant, certaines données de la procédure peuvent trouver une protection soit du fait de leur nature qui leur assure une protection particulière, soit parce que la procédure elle-même est soumise à une exigence de confidentialité se traduisant par une dérogation au principe de

[945] Pour reprendre l'expression de B. Bouloc, Nécessité d'un fait matériel en matière de recel, *RSC*, 1996, p. 645.
[946] Cass., crim., 6 mars 2012, *pourvoi* n°11-80.801. Il s'agissait en l'espèce de la révélation par un journaliste de données médicale concernant un sportif.
[947] Cass., crim., 9 juin 2015, *pourvoi* n°14-80.713. S'agissant en l'espèce de la diffusion par un journaliste d'un portrait-robot de suspect, la Cour a considéré qu'au vu de sa nature confidentielle, le document n'avait pas pu être transmis par une personne qui ne serait pas dépositaire du secret. Dans cet arrêt, la Cour de cassation a utilement rappelé que les dispositions de l'article 35 de la loi du 29 juillet 1881 qui permettent de produire en justice des éléments issus d'une violation du secret de l'instruction ne s'appliquent qu'au cas où la personne, prévenue, présente ces documents afin d'apporter la preuve de sa bonne foi ou du fait diffamatoire. En l'espèce, ces arguments n'étaient pas recevables. Voir à ce sujet, S. Lavric, Recel de violation du secret de l'instruction : quelques rappels, *Dalloz actualité*, 24 juin 2015.

publicité. Il convient donc de distinguer la protection directe attachée au caractère confidentiel des données (§1.) de la protection indirecte résultant de l'absence de publicité procédurale (§2.).

§1. La protection directe attachée au caractère confidentiel des données

324. Protection directe – Le caractère confidentiel de certaines données justifie une protection de celles-ci qui se manifeste par l'interdiction de communiquer des données couvertes par un secret professionnel (A.) ou par une anonymisation du témoignage (B.).

A. L'interdiction de communiquer des données couvertes par un secret professionnel

325. Secrets professionnels – Les secrets professionnels trouvent leurs sources dans divers textes mais leur violation relève dans tous les cas des dispositions de l'article 226-13 du code pénal. Les textes fixant le secret et ses modalités d'application et éventuellement de levée peuvent relever de règlements. De cette ambigüité découle en partie la complexité qui entoure la question de la levée du secret professionnel. Dans certains cas, le dépositaire du secret ne peut pas révéler les données en sa possession. Il s'agit ici de l'application même du principe de secret professionnel qui impose au professionnel de garder le silence. L'approche de cette question appelle dans un premier temps à s'interroger sur le caractère absolu ou relatif du secret professionnel (1°) pour appréhender les cas dans lesquels est faite une application stricte du principe (2°).

1° Le caractère relatif ou absolu du secret

326. Portée du secret – Il est depuis longtemps fait référence dans la jurisprudence au caractère absolu de certains secrets. La doctrine a souvent opéré une distinction entre secret absolu et secret relatif. Dans une certaine approche de la question, le secret absolu est présenté comme celui qui reste opposable face à la justice là où le secret relatif est amené à être levé[948]. Ainsi, le secret professionnel apparait comme ayant un caractère absolu lorsqu'il est opposé

[948] Voir, B. Py, *Secret professionnel*, Revue de droit pénal et de procédure pénale, Février 2003, actualisé mai 2020, 95.

aux personnes privées et relatif lorsqu'il est opposé aux personnes publiques[949]. « L'intensité du secret »[950] a pu aussi être présentée comme étant fonction de la possible dispense de témoigner qui y est attachée. Partant de ces postulats, le secret professionnel liant l'avocat et son client est relatif puisque ce dernier peut dans certains cas faire état de correspondances échangées avec son client[951]. *A contrario,* le secret médical apparait comme absolu, ne laissant au médecin aucune possibilité de se voir dispensé de son obligation de garder le silence. Une autre approche consiste à observer l'intérêt en jeu[952]. Par exemple, le notaire qui serait appelé à témoigner dans une instance civile pourrait opposer le secret professionnel. Le procès civil portant sur des intérêts individuels, il n'y a pas lieu de déroger au secret[953]. A l'inverse, le notaire témoin dans une affaire pénale peut être dans l'obligation de révéler certaines données en sa possession, la procédure pénale touchant l'intérêt général[954]. Avec la consécration du droit à la preuve[955], une approche suggère de distinguer les secrets professionnels répondant à « un motif d'intérêt général impérieux » qui seraient absolus en ce sens qu'ils ne pourraient céder que si la loi le prévoit, et les secrets professionnels fondés sur le respect de la vie privée qui devraient toujours faire l'objet d'une conciliation avec le droit à la preuve[956]. Il s'agirait donc d'une appréciation au cas par cas de la mise en balance d'un côté de la protection des données couvertes par le secret et de l'autre du droit à la preuve nécessitant la levée du secret en question.

327. La levée du secret attachée à la nature de la donnée – Au regard des questions intéressant les données à caractère personnel et notamment des lois adoptées récemment tant au niveau supranational qu'interne, on peut envisager une approche qui serait fonction de la nature des données dont la communication est nécessaire à l'instance. Il conviendrait donc de distinguer parmi les données couvertes par le secret celles qui sont de nature sensibles au sens de la loi informatique et liberté et les autres. Partant de là, on peut par exemple considérer que les données couvertes par le secret médical sont par principe susceptibles de constituer des

[949] M. Bénéjat, *Que reste-t-il du secret professionnel du notaire ?, in*, La responsabilité de l'avocat et du notaire, Travaux de l'Institut de sciences criminelles et de la justice, n°3, Cujas, 2013, p. 66.
[950] C. Guéry, P. Chambon, *Droit et pratique de l'instruction préparatoire*, *op. cit*.
[951] Voir *infra*
[952] Pour reprendre la présentation faite par B. Py, *Secret professionnel*, Revue de droit pénal et de procédure pénale, *op. cit*., 98.
[953] Cass., civ. 1ère, 27 novembre 1928.
[954] CA Paris, 13 juillet 1973, D.1974.16. Cass., civ 1ère., 20 juillet 1994, *pourvoi* n°92-21.615. Ce raisonnement est repris concernant le secret bancaire dans l'arrêt de la chambre commerciale de la cour de cassation en date du 13 juin 1995 (*pourvoi* 93-16.317).
[955] Cass., civ 1ère, 5 avril 2012, *pourvoi* n° 11-14.177.
[956] G. Lardeux, *Preuve*, Répertoire de droit civil, *op. cit*., 377.

données sensibles même si l'on peut imaginer qu'un médecin soit amené à divulguer des données qui bien que couvertes par le secret ne soient pas sensibles. Finalement, cette approche n'enferme pas le secret dans une dichotomie absolu ou relatif en fonction du professionnel qui en est dépositaire mais s'attache à la nature des données traitées. Ainsi, se rapprochant du raisonnement précédent, la levée du secret qui toucherait aux données sensibles aurait intérêt à être encadrées par la loi, pour le reste une mise en balance avec le droit à la preuve permettrait d'appréhender les différents intérêts en présence. Cette approche soulève néanmoins la question de savoir s'il faut se placer du côté de celui qui a intérêt à ce que le secret soit levé ou du côté de celui à qui profite le secret ? L'étude de la jurisprudence permet difficilement de dégager une quelconque théorisation à ce sujet. Néanmoins, il apparait que certains secrets demeurent plus absolus que d'autres, ce qui apporte apportant des éléments de réponse.

2° L'application stricte du principe de secret

328. Une application stricte du secret s'agissant du dossier médical – Le secret médical intéresse particulièrement la question du traitement des données à caractère personnel. Les données médicales sont susceptibles de constituer des données personnelles sensibles au sens de la loi informatique et liberté. Si la loi informatique et liberté encadre le traitement de telles données[957], ces données sont couvertes par le secret professionnel. Ce dernier est inscrit à l'article R4127-4 du code de la santé publique qui dispose que *« Le secret professionnel institué dans l'intérêt des patients s'impose à tout médecin dans les conditions établies par la loi. Le secret couvre tout ce qui est venu à la connaissance du médecin dans l'exercice de sa profession, c'est-à-dire non seulement ce qui lui a été confié, mais aussi ce qu'il a vu, entendu ou compris »*. Le secret médical a été qualifié de secret absolu[958]. Ce caractère a pu être affirmé notamment lorsque les juges ont estimé que le consentement du patient ne suffit pas à délier le médecin de son obligation. Ce raisonnement se retrouve dans un arrêt du Conseil d'Etat du 26 septembre 2018[959]. Le Conseil d'Etat rappelle ici que le simple consentement donné par le patient ne suffit pas à délier le médecin du secret professionnel, il convient que cette dérogation soit prévue par les textes. L'importance accordée au secret médical a été

[957] Le traitement peut être autorisé si le consentement de la personne intéressée est obtenu, ou s'il en va de l'intérêt public par exemple.
[958] Ce caractère est néanmoins discutable. V. *infra* n°
[959] CE, 4e et 1ère ch. réunies, 28 septembre 2018, n°497856.

rappelée par la Cour de cassation dans un arrêt du 28 juin 2012[960]. L'arrêt est particulier puisque les faits portent sur la révélation par un avocat de données médicales confiées par son client. Bien qu'ayant révélé ces données médicales dans l'intérêt de son client pour les « strictes exigences de sa propre défense »[961], la Cour de cassation rappelle que la divulgation de telles données est subordonnée au consentement de la personne intéressée. En soit, le litige ne porte pas directement sur la question de la violation du secret médical puisque les données ont été révélées par l'avocat invoquant un fait justificatif. Mais à cette occasion, la Cour de cassation rappelle que s'agissant des données médicales le consentement est nécessaire[962]. La jurisprudence civile semble également attacher la révélation de données médicales au consentement préalable de l'intéressé quand bien même la divulgation du dossier médical est requise dans le cadre d'une demande d'expertise[963].

Le secret professionnel conduit a une protection directe du fait du contexte dans lequel les données sont confiées par l'intéressé à l'individu soumis au secret. Cette protection peut également passer par l'anonymisation des certaines données notamment s'agissant du témoignage.

B. La protection par l'anonymisation du témoignage

329. La reconnaissance du statut de témoin anonyme – Le témoignage anonyme relève de dispositions particulières de la loi. Il faut exclure de ce statut les simples informations qui peuvent être portées à la connaissance des autorités anonymement et ouvrir potentiellement

[960] Cass., civ. 1ère, 28 juin 2012, *pourvoi* n°11-14.486.

[961] Tel que l'autorise l'article 4 du décret 2005-790 du 12 juillet 2005 relatif aux règles de déontologie de la profession d'avocat.

[962] G. Lardeux, *Preuve*, Répertoire de droit civil, octobre 2018, *op. cit*., 365. L'auteure adopte ici une interprétation extensive du secret médical. S'appuyant sur la lettre de l'article L1110-4 du code de la santé publique *(« Toute personne prise en charge par un professionnel de santé, un établissement ou service, un professionnel ou organisme concourant à la prévention ou aux soins dont les conditions d'exercice ou les activités sont régies par le présent code, le service de santé des armées, un professionnel du secteur médico-social ou social ou un établissement ou service social et médico-social mentionné au I de l'article L. 312-1 du code de l'action sociale et des familles a droit au respect de sa vie privée et du secret des informations la concernant »*.), elle considère que *« Les informations médicales ne changeant pas de nature lorsqu'elles sont détenues par une personne autre que celles tenues au secret médical, celui-ci s'impose à quiconque les aurait en sa possession »*.

[963] Cass., civ. 1ère, 15 juin 2004, *pourvoi* n°01-02.338. Cass., civ. 1ère, 11 juin 2009, *pourvoi* n°08-12.742. Néanmoins, si les données constituent un élément de preuve essentiel à l'issue du litige, le secret médical ne peut être opposé à l'expert (Cass., civ. 2ème, 22 novembre 2007, *pourvoi* n°06-18.250). Voir sur la question, V. Peltier Révélation d'une information à caractère secret, *JurisClasseur pénal*, Fasc. 30, 28 mai 2015.

une enquête, mais qui constituent de « simples renseignements »[964]. Le statut de témoin anonyme confère une protection particulière à l'individu. Initialement, cette mesure a pu se développer s'agissant des agents infiltrés ou indicateurs afin de permettre aux autorités d'accéder aux informations nécessaires à leur enquête, sans que les individus ne craignent des représailles. Fixé initialement par la loi du 15 novembre 2001[965], modifiée à plusieurs reprises, le statut de témoin anonyme permet, dans un premier temps, avec l'autorisation du procureur de la République ou du juge d'instruction, au témoin de ne pas divulguer son adresse[966]. Aussi, en cas de procédure portant sur un crime ou délit puni d'au moins trois ans d'emprisonnement et lorsque l'audition présente une menace pour la personne ou ses proches, le juge des libertés et de la détention peut permettre au témoin de s'exprimer sous couvert d'anonymat. Ainsi, l'identité du témoin n'apparaitra pas dans le dossier de procédure[967]. La loi du 3 juin 2016 renforçant la lutte contre le crime organisé est allée plus loin dans le dispositif prévoyant la possibilité pour les témoins, dans les procédures portant sur des crimes ou délits graves, de témoigner sous couvert d'anonymat en cas de menace pour leur intégrité physique. Codifié aux articles 706-62-1 et 706-62-2 du code de procédure pénale, ce dispositif permet au juge d'instruction ou président de juridiction, d'office ou sur demande du procureur de la République, d'ordonner que l'identité du témoin ne soit mentionnée ni au cours de l'audience, ni dans les ordonnances, jugements ou arrêts[968]. Cette procédure permet aussi le recours dans les mêmes conditions à une identité d'emprunt[969]. Ce régime de protection est justifié par la volonté d'assurer la protection des individus amenés à témoigner et celle leurs proches s'il y a une menace pour leur intégrité. Il s'agit donc d'assurer une protection renforcée de la vie privée des personnes afin de permettre leur témoignage dans une procédure quel qu'en soit le stade. Le dispositif assure donc la protection des données identifiantes. La question intéresse donc particulièrement le sujet puisque ces dispositions permettent de masquer l'identité d'un individu dans une procédure qui se veut par principe contradictoire et publique.

[964] Cass., crim., 9 juillet 2003, *pourvoi* n°03-82.119.
[965] Loi 2001-1062 du 15 novembre 2001relative à la sécurité quotidienne. Modifiée par la loi 2002-1138 du 9 septembre 2002, d'orientation et de programmation pour la justice et complétée par l'ordonnance 2019-964 du 18 septembre 2019 prise en application de la loi n° 2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice.
[966] Art. 706-57 du code de procédure pénale.
[967] Art. 706-58 du code de procédure pénale.
[968] Art. 706-62-1 du code de procédure pénale.
[969] Art. 706-62-2 du code de procédure pénale.

330. Les interrogations soulevées par le recours au témoignage anonyme – Le recours au statut de témoin anonyme n'est pas sans soulever de vives interrogations. La doctrine rappelle utilement l'importance du nom et de l'identité dans les procédures à travers notamment l'incrimination d'usurpation d'identité[970]. En effet, on peut s'interroger sur les conséquences de l'anonymat du témoignage au regard de l'importance dans le droit interne de l'identificabilité de l'individu au cours de la procédure. En matière pénale, l'article 706-62 du code de procédure dispose qu'aucune condamnation ne peut être fondée sur des déclarations obtenues sous couvert d'anonymat dans les conditions prévues aux articles 706-58 et 706-61 du code de procédure pénale, rejoignant la position de la Cour européenne des droits de l'homme[971]. La Cour de cassation a apporté des précisions en considérant que les informations obtenues par un policier auprès d'un individu souhaitant rester anonyme ne constituent pas un procès-verbal de témoignage anonyme mais permettent de dresser un procès-verbal de renseignements qui ne peut servir de preuve[972].

Ainsi, que ce soit au nom du caractère secret des données visées ou par la nécessité d'anonymiser un témoignage, ces procédés constituent des atteintes au principe du contradictoire. Dans le premier cas, c'est la nature même de la donnée qui nécessité qu'il soit fait obstacle au contradictoire. Dans le second cas, il s'agit de masquer l'identité et donc les données à caractère personnel de l'individu afin d'assurer une protection renforcée, portant de facto atteinte au contradictoire. Lors de l'audience, le secret constitue également l'exception dans une procédure par principe publique.

331. Le rejet du témoignage anonyme en matière civile – Dans un arrêt récent, la Cour de cassation s'est prononcée sur la question s'agissant de la matière civile. La chambre sociale a jugé que le licenciement fondé sur un rapport de la commission d'éthique non signé et comportant des témoignages anonymes contrevient aux principes du procès équitable[973]. La Cour de cassation a considéré que l'individu visé par le licenciement aurait du, afin d'assurer sa défense, avoir connaissance de l'identité des témoins. On retrouve ici la limite, posée par ailleurs en procédure pénale, en vertu de laquelle dans certains cas la révélation de l'identité

[970] J. Le Calvez, Les dangers du « X » en procédure pénale : opinion contre le témoin anonyme, *Dalloz*, 2002, p.3024.
[971] La Cour E.D.H. vise elle le « fondement déterminant ».
[972] Cass. crim., 9 juillet 2003, *pourvoi* n°03-82.119. La Cour de cassation considère que les informations obtenues par un policier auprès d'un individu souhaitant rester anonyme ne constituent pas un procès-verbal de témoignage anonyme mais permettent de dresser un procès-verbal de renseignement qui ne peut servir de preuve.
[973] Cass., soc., 4 juillet 2018, *pourvoi* n°17-18.241. Voir, J. Mouly, Témoignages anonymes et droits de la défense du salarié, *Droit social*, 2018, 951.

du témoin est nécessaire au vu des circonstances[974]. Cette solution rendue en matière civile est néanmoins inédite. Elle renvoie à un point soulevé par la doctrine qui veut que l'identificabilité du témoin permet d'accorder une certaine fiabilité au témoignage[975] et donc de garantir les droits de la défense. En effet, la connaissance de l'identité du témoin peut permettre de comprendre le lien qu'il peut entretenir avec la victime par exemple ce qui peut dans une certaine mesure avoir une importance dans l'appréciation faite du témoignage[976].

§2. La protection indirecte résultant de l'absence de publicité

332. Protection indirecte – Les données de procédure peuvent bénéficier d'un régime particulier du fait notamment de l'absence de publicité des débats ou du jugement qui par conséquent offrent une protection indirecte des données. Ainsi, les débats (A.) et les jugements tenus non publiquement (B.) peuvent s'analyser comme protecteurs des données de la procédure.

A. Les débats tenus non publiquement

333. Huis-clos et débats en chambre du conseil – Il existe des exceptions au principe de publicité tant en procédure pénale que civile. Ces exceptions visent notamment les débats, le prononcé du jugement ne connaissant que de très rares exceptions. Le huis-clos peut être ordonné dans certains cas en raison de la nature de l'infraction ou de la menace pesant sur l'ordre ou les mœurs. Il peut également n'être que partiel et ne viser qu'une partie de l'audience ou qu'une catégorie de personnes[977]. En matière civile, par exception au principe de publicité, les débats peuvent se tenir en chambre du conseil en fonction de la nature du contentieux. Une exception à la publicité peut être ordonnée pour différents motifs.

[974] Art. 706-60 du code dé procédure pénale.
[975] J. Le Calvez, Les dangers du « X » en procédure pénale : opinion contre le témoin anonyme, *op. cit.*, p.3024. L'auteur va plus loin dans son raisonnement soulevant la question de « l'altération sensible » potentielle à l'intime conviction du fait d'une hiérarchisation des preuves liée au recours à l'anonymat du témoin. Aussi, l'auteur considère que malgré ce dispositif les questions posées à l'audience peuvent être de nature à rendre le témoin identifiable, soulevant la question du bien-fondé et de la nécessité de maintenir ce régime. L'auteur soulève également la question de la validité de ce dispositif avec le droit posé par la Convention européenne des droits de l'homme pour toute personne poursuivie de faire interroger les témoins à charge, nécessitant donc de lever l'anonymat.
[976] Le juge qui ordonne l'anonymat a néanmoins pour sa part connaissance de l'identité du témoin qui prête serment, ce qui se conforme à la position de la Cour européenne des droits de l'homme.
[977] Cass., crim., 23 février 1966, *pourvoi* 65-CS-111.

L'exception à la publicité peut être prononcée en cas de menace pour l'ordre public (1°), menace pour des intérêts privés (2°) ou être fonction de la nature du contentieux (3°).

1° L'exception à la publicité en cas de menace pour l'ordre public

334. Ordre public et publicité – Les articles 306 du code de procédure pénale et 400 alinéa 2 du code de procédure pénale prévoient la possibilité qu'il soit dérogé au principe de publicité des débats en cas de menace pour l'ordre, la moralité[978] ou la sécurité publique. La Cour de cassation est, à l'occasion d'un récent arrêt, revenue sur la notion même d'ordre tel que visée dans l'article 306 du code de procédure pénale apportant ainsi des précisions utiles. Dans cet arrêt en date du 20 février 2019[979], la Cour de cassation opère une distinction entre les faits susceptibles de créer un danger pour l'ordre et les troubles à l'ordre causés par des personnes assistant à l'audience. Dans le premier cas de figure, le président de la Cour d'assises peut ordonner le huis-clos sous couvert de l'article 306 précité. Toutefois, si le trouble est causé par l'attitude de personnes présentes à l'audience, alors le président peut user de son « pouvoir de police » et ordonner leur expulsion de la salle d'audience en vertu de l'article 321 alinéa 1er du code de procédure pénale[980]. Cette éventualité est prévue en matière pénale à l'article 404 du code de procédure pénale. En matière civile, on retrouve cette exception à l'article 435 du code de procédure civile qui prévoit en cas d'atteinte à la sérénité de la justice la possibilité d'expulser les perturbateurs. Toutefois, cette exception à la publicité ne touche pas outre mesure le sujet des données à caractère personnel au-delà du fait de limiter la publicité des données de l'audience.

2° L'exception à la publicité en cas de menace pour les intérêts privés

335. Menace pour les intérêts privés et publicité – Il peut être dérogé au principe de publicité afin d'assurer la protection des personnes. L'article 435 du code de procédure civile prévoit expressément la possibilité de mener les débats en chambre du conseil en cas de menace pour la vie privée. En matière pénale, l'article 400 du code de procédure pénale prévoit la possibilité des débats à huis-clos lorsque la publicité est susceptible de porter atteinte à la sérénité des débats, à la dignité des personnes ou les intérêts d'un tiers. L'article

[978] Par exemple, Cass., crim., 4 novembre 1999, *pourvoi* n°98-87.165.
[979] Cass., crim., 20 février 2019, *pourvoi* n°18-82.915.
[980] A. Lepage, Des restrictions qui peuvent être apportées à la publicité des débats devant la Cour d'assises, *Communication commerce électronique*, n°5, mai 2019, comm. 33.

402 du code de procédure pénale prévoit la possibilité d'interdire l'accès à la salle d'audience aux mineurs. Sur la question du huis-clos, la Cour européenne des droits de l'homme a considéré que les données médicales en tant que données protégées se rattachaient à la vie privée et justifiaient donc le huis-clos des débats[981]. Par la suite, cette dernière a affirmé que le secret professionnel ne pouvait pas écarter le principe de publicité[982]. Finalement, un décret du 5 février 1993[983] est venu poser le principe de publicité des audiences disciplinaires. Il appartient au président d'office ou sur demande des parties de prononcer le huis-clos pour motif d'ordre public, de protection de la vie privée ou de protection du secret médical. Le principe reste donc celui de la publicité. Dans un domaine plus spécifique issu de la loi du 30 octobre 2017 sur la sécurité intérieure, le huis-clos peut être ordonné afin d'assurer la protection d'un témoin ou de ses proches lorsque celui-ci est repenti[984]. Dans sa décision du 21 juillet 2017[985], le Conseil constitutionnel fait référence à la protection de la vie privée afin de justifier l'exception faire au principe de publicité.

3° L'exception à la publicité attachée à la nature du contentieux

336. L'exception à la publicité sur demande des parties en matière criminelle – Il est admis en procédure pénale que le huis-clos puisse être demandé devant la Cour d'assises par la victime, partie civile, lorsqu'il s'agit d'une infraction de viol, de tortures ou d'actes de barbarie accompagnés d'agressions sexuelles, de traite des êtres humains ou de proxénétisme aggravé[986]. Ces dispositions visent à assurer la protection de la vie privée de la victime et pour cela le huis-clos ne peut être ordonné outre les cas précités que si celle-ci ne s'y oppose pas. A l'occasion d'une question prioritaire de constitutionnalité le Conseil constitutionnel a eu à se prononcer sur la compatibilité de ces dispositions avec le principe de publicité des débats. Dans une décision du 21 juillet 2017[987], ce dernier a considéré qu'en permettant à la seule victime partie civile de demander le huis-clos, le législateur protégeait entre autre sa vie privée, limitant ainsi la probabilité que cette dernière ne renonce à dénoncer les faits. Le

[981] Cour E.D.H., 2 juillet 1990, *Guenoun c/ France*, 66-181, 13-562/88.
[982] Cour E.D.H., 26 septembre 1995, *Diennet c/ France*, 18160/91.
[983] Décret, 93-181 du 5 février 1993, modifiant le décret n° 48-1671 du 26 octobre 1948 modifié relatif au fonctionnement des conseils de l'ordre des médecins, des chirurgiens-dentistes et des sages-femmes et de la section disciplinaire du Conseil national de l'ordre des médecins.
[984] Art. 706-63-2 du code de procédure pénale.
[985] Cons. Const., n°201-645 QPC. Voir par exemple, M. H. Yazici, Conformité constitutionnelle du huis clos de droit à la demande de la partie civile, *Dalloz Actualité*, 13 septembre 2017.
[986] Art. 306 du code de procédure pénale
[987] Cons. Const., n°201-645 QPC.

Conseil constitutionnel considère alors que ces dispositions protègent l'intérêt général et sont conformes au principe de publicité et à la jurisprudence antérieure[988].

337. Les débats en chambre du conseil en matière familiale – L'article 1074 du code de procédure civile prévoit que les débats en matière familiale se déroulent en chambre du conseil. Cette absence de publicité est d'ordre public et doit donc s'appliquer sous peine de nullité de la procédure[989]. La Cour européenne des droits de l'homme s'est prononcée sur la question de la conformité de ces dispositions au regard des droits fondamentaux. Le requérant invoquait en effet une violation des droits de la défense et demandait la publicité des débats ainsi que du prononcé de la décision. La Cour européenne a rappelé à cette occasion que l'article 6§1 prévoit la possibilité d'interdire à certaines personnes ou à tout public l'accès à la salle d'audience lors des débats notamment pour des motifs d'ordre public, de sécurité nationale ou de protection de la vie privée. Sans surprise, la Cour considère que les dispositions litigieuses ne méconnaissent pas la Convention[990].
S'il existe finalement de nombreuses justifications permettant de faire exception à la publicité des débats, il y a peu d'exceptions à la publicité du jugement.

B. Les jugements rendus non publiquement

338. L'admission de l'exception au principe de publicité du jugement – Les dispositions légales internes prévoient peu d'exceptions au principe de publicité du jugement. Ces exceptions reposent sur la nature du contentieux qui peut justifier que le jugement ne soit rendu publiquement comme en matière d'assistance éducative par exemple[991]. Si l'article 6§1 de la Convention européenne des droits de l'homme ne prévoit pas, non plus, explicitement de dérogations au principe de publicité du jugement, la Cour européenne a fait le choix d'une interprétation des dispositions au regard de la nature du jugement. Aussi, dans certaines matières elle considère que la publicité n'est pas nécessaire comme en matière civile gracieuse ou en matière de jugement intéressant l'état des personnes.

[988] Dans un arrêt du 3 avril 1996, la chambre criminelle a considéré que les dispositions de l'article 306 al 3 du code de procédure pénale entrent dans les prévisions de l'article 6.1 de la CEDH (Cass., crim., 3 avril 1996, pourvoi n°95-83.366)
[989] V. Bonnet, A. Gouttenoire, *Divorce, procédure – Exercice de l'action en divorce*, Répertoire de procédure civile, juillet 2017.
[990] Cour E. D. H., 29 avril 2001, *B. et P. c/ Royaume-Uni*, 36337/97;35974/97.
[991] Art. 1189 al 3 du code de procédure civile.

La loi du 23 mars 2019 de réforme pour la justice va dans ce sens en précisant explicitement que le principe de publicité des jugements ne s'applique pas en matière gracieuse, en matière d'état des personnes et de capacité, dans les matières intéressant la vie privée et dans les matières intéressant le secret des affaires[992]. Le Conseil constitutionnel a validé ces dispositions lors d'un contrôle a priori. Dans une décision du 21 mars 2019, il a pour la première fois, reconnu la valeur constitutionnelle du principe de publicité en matière civile[993], décidant que les dispositions ne méconnaissent pas le principe d'égalité devant la loi et d'accès au service public de la justice ni l'article 34 de la Constitution.

A l'inverse des cas justifiant la mise en œuvre de mesures visant directement ou indirectement la protection des données de la procédure, certaines données font au contraire l'objet d'une communication. Certains principes justifient la diffusion de données qui est nécessaire au déroulement de la procédure.

[992] Loi n°2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice, Art 33.
[993] Cons., const., 2019-79 DC du 21 mars 2019, cons. 105.

CHAPITRE 2 : LES PRINCIPES JUSTIFIANT LA DIFFUSION DE DONNEES

339. Diffusion des données de procédure – Le déroulement procès suppose la communication des données de procédure entre les parties elles-mêmes et entre les parties et le juge. Cette diffusion des données de procédure peut découler de l'application de principes procéduraux impliquant l'obligation de communiquer ou résulter, par extension, de règles plus particulières. Il convient donc d'aborder les questions attachées à la diffusion des données découlant de l'application des principes généraux (Sect. 1) puis d'adopter une approche extensive s'agissant de la diffusion des données (Sect. 2).

Section 1 : La diffusion de données découlant de l'application de principes généraux

340. Diffusion conséquence de principes généraux – Les principes généraux régissant la diffusion des données de procédure renvoient d'abord au principe du contradictoire qui impose de communiquer les données aux autres parties. Ensuite, ces principes impliquent la diffusion publique des données par l'application du principe de publicité. Ces deux principes procéduraux induisent des conséquences très différentes et donc des interrogations également très distinctes. En effet, le champ de diffusion n'est pas similaire selon que la diffusion relève de l'application du contradictoire ou du principe de publicité. Il convient donc d'aborder le sujet sous deux angles avec les données communiquées par l'application du contradictoire (§1.) et les données diffusées par l'application du principe de publicité (§2.).

§1. Les données communiquées par l'application du contradictoire

341. Portée du contradictoire – Souvent présenté comme un corollaire des droits de la défense et notamment du droit au procès équitable, le principe du contradictoire intéresse nécessairement la question du traitement des données à caractère personnel dans le procès puisqu'il impose que soient communiquées aux autres parties toutes les pièces versées au dossier. Une brève étude du principe et de sa portée (A.) permet d'en mesurer les enjeux en termes de traitement de données à caractère personnel, notamment s'agissant des données d'expertises (B.).

A. La portée du principe de la contradiction

342. Principe du contradictoire – En matière pénale comme civile, le principe du contradictoire a pour conséquence la communication des pièces du dossier de procédure. Qualifié souvent de droit naturel (1°), il apparait comme l'affirmation d'un droit à l'information (2°).

1° Un droit naturel

343. Un droit « naturel » – Il est souvent admis que le principe du contradictoire trouve sa source dans celui des droits de la défense et du droit au procès équitable même s'il n'y est pas fait expressément référence dans l'article 6§1 de la convention européenne des droits de l'homme[994]. Il a pu être présenté comme un droit « naturel » car il repose sur l'idée de « *respect des arguments des autres, donc nécessité de les connaitre par communication des pièces* » et parce que « *le procès doit déboucher sur une vérité […] c'est par la contradiction que le juge est amené à dégager cette vérité* »[995]. Le contradictoire se trouve érigé en droit fondamental du procès tant dans la matière civile que pénale. La bonne administration de la justice a été reconnue comme un objectif à valeur constitutionnelle dans une décision du 3 décembre 2009[996]. Le Conseil constitutionnel rapproche le principe du contradictoire des notions de communication de pièces et d'équilibre des droits des parties[997]. Le principe du contradictoire a été érigé en principe général du droit et principe directeur du procès. Dans un premier temps, le Conseil d'Etat a reconnu comme principes généraux du droit, les droits de la défense[998] et plus particulièrement le droit à une procédure contradictoire[999]. Pour la Cour européenne des droits de l'homme le contradictoire « implique par principe, pour une partie, la faculté de prendre connaissance des observations ou des pièces produites par l'autre, ainsi

[994] L.A. Sicilianos, M.A. Kostopoulou, *Conv. E.D.H. art. 6 : la protection du droit à un procès équitable dans la jurisprudence de la Cour européenne des droits de l'homme,* Répertoire de droit européen, janvier 2018 actualisation février 2020, 97, 98. A. Cappello, Question prioritaire de constitutionnalité, Impact de la question prioritaire de constitutionnalité sur la matière pénale, *Répertoire de droit pénal et de procédure pénale*, n°257, juin 2015, actualisation décembre 2017. Selon l'auteure, cette appartenance du principe du contradictoire aux droits de la défense n'est pas « certaine ».
[995] S. Guinchard, *Droit processuel : droits fondamentaux du procès*, 10 ed, Dalloz, 2019, p.1122.
[996] H. Apchain, Retour sur la notion de bonne administration de la justice, *AJDA*, 2012, 587.
[997] En ce sens, A. Cappello, *Question prioritaire de constitutionnalité – Impact de la QPC sur la matière pénale, op. cit.*, n°259.
[998] CE, Sect., 5 mai 1944, Veuve Trompier-Gravier, 69751.
[999] CE, Ass., 16 janvier 1976, Gate, 94150. CE, Ass., 12 octobre 1979, Rassemblement des nouveaux avocats. T. Grundler, Le droit au recours confronté au secret, *AJDA*, 2009, 2358.

que de les discuter »[1000]. Cette dernière faisant directement référence au « droit à un procès équitable contradictoire »[1001]. La Cour de justice de l'Union européenne a, quant à elle, qualifié le principe du contradictoire de « principe fondamental du droit communautaire »[1002]. Aussi, le principe du contradictoire s'est vu érigé en principe fondamental reconnu par les lois de la République[1003]. Le Conseil constitutionnel va par la suite, de manière plus générale, reconnaitre une valeur constitutionnelle aux droits de la défense[1004].

« Le principe de l'égalité des armes fait partie intégrante de la notion du procès équitable. Ce principe ainsi que celui du contradictoire couvrent l'ensemble du droit procédural »[1005]. Le principe d'égalité des armes s'applique tant à la matière civile que pénale et implique donc que toutes les parties soient en mesure de se défendre dans « un juste équilibre »[1006]. Le principe du contradictoire peut en ce sens être présenté comme un principe « autonome » complémentaire de celui d'égalité des armes qui garantit également un procès équitable[1007]. La Cour européenne des droits de l'homme opère toujours une appréciation *in concreto* du respect du contradictoire. Dans l'arrêt *Muncaciu c /Roumanie* du 26 janvier 2016, la Cour rappelle que « *dans la mesure où l'article 6§ 1 de la Convention vise avant tout à préserver les intérêts des parties et ceux d'une bonne administration de la justice […] la cause du requérant n'a pas été entendue équitablement, faute de débat contradictoire dans la procédure de recours* »[1008]. En cela, on peut considérer que le principe du contradictoire sert la cause plus générale de bonne administration de la justice.

344. Une notion empreinte d'incertitudes – Le principe du contradictoire revêt deux volets. Il renvoie à « l'accès aux éléments sur lesquels le juge est susceptible de fonder la décision [et] doit permettre [aux] parties de discuter de tous ces éléments dans la perspective de la

[1000] Cour E. D. H., 26 juin 1993, *Ruiz-Mateos c/ Espagne*, 12952/87, §63. CEDH 7 juin 2001, *Kress c/ France*, §74. Ce raisonnement fait lui-même écho à celui que la Cour avait eu en 1991 dans l'arrêt du 28 aout, *Brandstetter c/ Autriche*. Dans cet arrêt, la Cour faisait référence au caractère nécessairement contradictoire de la procédure pénale au nom du droit au procès équitable et du principe d'égalité des armes.
[1001] Cour E. D. H., 24 février 1995, *Mc Michael c/ Royaume-Uni*, 16424/90.
[1002] Cour J. C. E., 31 mars 1993 *A. Ahlström Osakeyhtio et autres c/ Commission*, C89/85.
[1003] Conseil Const., 2 décembre 1976, 76-70 DC.
[1004] Conseil Const., 13 aout 1993, 93-325 DC.
[1005] L.A. Sicilianos, M.A. Kostopoulou, *Conv. EDH art 6 : La protection du droit à un procès équitable dans la jurisprudence de la Cour européenne des droits de l'homme*, *op. cit*., 97.
[1006] Conv E.D.H., 2 octobre 1993, *Dombo beheer B.V. c/ Pays-Bas*, 14448/88, §33.
[1007] En ce sens, L.A. Sicilianos, M.A. Kostopoulou, *Conv. EDH art 6 : La protection du droit à un procès équitable dans la jurisprudence de la Cour européenne des droits de l'homme*, Répertoire de droit européen, *op. cit*., 97. Conv. E.D.H., 19 décembre 1989, *Kamasinski c/ Autriche*, 9783/82 ; §102.
[1008]Cour E.D.H., 26 janvier 2016, *Muncaciu c/ Roumanie*, 12433/11, §46.

défense de leurs intérêts »[1009]. Si le principe est souvent présenté comme découlant du principe plus général de droit au procès équitable leurs champs d'application ne se confondent toutefois pas. Cela a pu conduire une partie de la doctrine à y voir une notion « incertaine » et dont « l'appartenance aux droits de la défense n'est pas certaine »[1010]. Cette position peut être discutée et ce raisonnement impliquerait quoi qu'il en soit de s'interroger en amont sur la notion même de droits de la défense qui peut elle-même soulever des interrogations[1011]. Ainsi, le sujet ouvre la question de savoir si le principe du contradictoire est un droit autonome[1012]. Ces différentes approches permettent de comprendre les interrogations qui entourent la notion même du principe de contradictoire.

2° Le contradictoire comme affirmation d'un droit à l'information

345. Le principe du contradictoire comme affirmation d'un droit à l'information – L'idée selon laquelle le principe du contradictoire repose sur un droit à être informé n'est pas récente. Dès 1991 la Cour européenne des droits de l'homme a considéré qu'au nom du contradictoire l'accusé devait pouvoir s'exprimer après le dépôt des conclusions de l'avocat général bien que celui-ci ne soit pas partie au procès[1013]. La Cour européenne des droits de l'homme a affirmé que le fait pour une partie à l'instance de ne pas avoir connaissance de l'avis rendu par le ministère public et de ne pas pouvoir y répondre constitue une violation du principe du contradictoire[1014]. On retrouve également ce raisonnement dans les considérants

[1009] A. Gouttenoire, Le principe du contradictoire devant la Cour européenne des droits de l'homme, in *Le contradictoire dans le procès pénal – nouvelles perspectives,* Cujas, 2012, p. 65.
[1010] A. Cappello, *Question prioritaire de constitutionnalité – Impact de la QPC sur la matière pénale*, Répertoire de droit pénal et procédure pénale, *op. cit.*, n°257.
[1011] Voir sur la question, Y. Capdepon, *Essai d'une théorie générale des droits de la défense*, *op. cit*.
[1012] Voir, Y. Strickler, *Principe de la contradiction*, Jurisclasseur procédure civile, Fasc. 500-40, 1er décembre 2018. L'auteur présente le principe du contradictoire comme un « moyen technique permettant d'assurer les droits de la défense et de les mettre en œuvre » et donc comme découlant des droits de la défense. Ce dernier semble alors aller dans le sens de la Cour européenne des droits de l'homme selon laquelle le contradictoire est « le droit de se voir communiquer et de discuter toute pièce ou observation présentée au juge, fût-ce par un magistrat indépendant, en vue d'influencer sa décision » (Conv. E.D.H., 27 mars 1998, J.J. c/ Pays-Bas.). Voir aussi l'arrêt Messier contre France dans lequel la Cour affirme que « Tout procès pénal, y compris ses aspects procéduraux, doit revêtir un caractère contradictoire et garantir l'égalité des armes entre l'accusation et la défense : c'est là un des aspects fondamentaux du droit à un procès équitable», (Cour E.D.H., 30 juin 2011, Messier c/ France.). Enfin, l'arrêt *Vidal contre Belgique* est un exemple des arrêts dans lesquels la Cour rattache le principe du contradictoire à celui d'égalité des armes. Recherchant si la procédure avait été équitable, la Cour va considérer qu'en écartant certains moyens de preuve pour fonder leurs décisions les juges n'avaient pas respecté le caractère contradictoire de la procédure (Conv. E.D.H., 22 avril 1992 ; Vidal *c/ Berlgique, 12351/86*.) Voir, L.E. Pettiti, Principe du contradictoire et égalité des armes, *RSC*, 1992, p. 798.
[1013] CEDH 30 octobre 1991, *Borgers c/ Belgique*, 12/00586. Dans cette affaire la CEDH a également condamné la pratique qui consistait pour l'avocat général à assister aux délibérés. Par la suite cette pratique a été condamnée en France (*Reinhardt et Slimane Kaïd* du 31 mars 1998 n°22921/93 et 23043/93).
[1014] Cour E.D.H., 20 févr. 1996, *Vermeulen c/Belgique*, req. no 19075/91.

de la Cour européenne notamment dans un arrêt du 27 mars 1998[1015]. Ce raisonnement repose sur l'idée selon laquelle tout justiciable partie dans une affaire doit être en mesure de discuter toutes les pièces du dossier et donc d'en avoir connaissance. La Cour européenne des droits de l'homme adopte une vision large du principe et considère qu'il doit s'appliquer à tous les stades de la procédure[1016]. Dans un arrêt récent, elle a condamné la Belgique en affirmant que le principe du contradictoire implique que les pièces du dossier soient communiquées aux parties mais que ce principe implique aussi le droit pour les parties d'avoir connaissance des observations de l'avocat général devant la Cour de cassation et donc soient informées suffisamment tôt de la date de l'audience pour être présentes[1017].

346. Fondements du contradictoire en matière pénale – En droit interne, le principe du contradictoire trouve à s'appliquer lors de la phase juridictionnelle[1018]. L'article 427 du code de procédure pénale dispose que l'administration de la preuve doit être contradictoire. Le droit interne semble donc exclure la phase d'enquête du champ d'application du contradictoire certains y voyant l'existence d'une inégalité[1019], néanmoins contrebalancée par le droit accordé au suspect de demander des mesures d'enquête complémentaires s'il l'estime utile.

La loi du 27 mai 2014[1020] transposant de la directive du 22 mai 2012 visant à renforcer le droit à l'information dans les procédures pénales va opérer un changement en affirmant un droit à l'information avant la phase du procès, certains la présentant même comme marquant « l'apogée du basculement de la garde à vue dans le contradictoire »[1021]. Il est désormais possible, pour la personne jugée en comparution immédiate à l'issue d'une garde à vue, d'être

[1015] Cour E.D.H., 27 mars 1998, J.J. c/ Royaume-Uni, 21351/93. La Cour fait référence à un droit à se voir communiquer toutes les pièces du dossier.

[1016] Cour E.D.H., 11 oct. 2012, *Abdelali* c/ *France*, n° 43353/07. La Cour européenne des droits de l'homme a également rappelé que le principe d'égalité des armes tend pour sa part à s'appliquer dès le stade de l'enquête.C.E.D.H. 11 juillet 2000, Dikme c/ Turquie, n°°20869/92.

[1017] Cour E.D.H., 22 oct. 2019, *Venet c/ Belgique*, n° 27703/16. En l'espèce, la date d'audience avait été notifiée tardivement au demandeur et ce dernier, incarcéré, n'avait pas pu assister à l'audience. Voir à ce sujet, F. Charlent, Principe du contradictoire et avis de l'avocat général à la Cour de cassation, *Dalloz actualité*, 5 novembre 2019. L'auteure fait utilement le parallèle entre le statut de l'avocat général en droit Belge et celui en droit français. Leur similitude permet a priori une transposition de cette décision en droit interne.

[1018] P. Gagnoud, Le renforcement du contradictoire dans la phase des poursuites : vers une mise en état des affaires pénales ?, *Gazette du palais*, n°214, p. 10. L'auteur rappelle utilement que dans le système français par tradition inquisitorial le contradictoire n'a pas sa place lors de la phase d'enquête. A ce stade les droits de la défense visent à garantir les libertés individuelles.

[1019] E. Daoud, A. Jacquin, L'effectivité du principe du contradictoire, AJ pénal, 2016, p. 112.

[1020] Loi n°2014-535 du 27 mai 2014 portant transposition de la directive 2012/13/UE du Parlement européen et du Conseil, du 22 mai 2012, relative au droit à l'information dans le cadre des procédures pénales.

[1021] G. Beaussonie, La nouvelle garde à vue est elle plus contradictoire ?, *Gazette du palais*, 29 juillet 2014, n°210, p. 13.

assisté d'un avocat lors de son déferrement devant le procureur de la République, et donc avant d'éventuelles poursuites par celui-ci, donnant ainsi accès au dossier avant la phase juridictionnelle[1022]. Ce droit à l'assistance d'un avocat ainsi que le droit de formuler des déclarations ou au contraire de garder le silence doit désormais être notifié à la personne. Ces dispositions redonnent au contradictoire une place importante avant même la phase de jugement et font du procureur de la République un acteur important de sa mise en œuvre[1023]. Il ne s'agit toutefois pas d'un droit d'accès illimité aux pièces du dossier et une partie de la doctrine a reproché au législateur une réforme timide en comparaison des avancées du droit européen[1024]. De la même manière le droit à l'assistance d'un avocat et les modalités d'accès au dossier sont désormais explicitement mentionnés dans les convocations[1025], fixant même des délais dans lesquels le dossier doit être transmis[1026]. La loi prévoit également, dans le cas où la convocation intervient moins de deux mois avant l'audience et lorsque le dossier n'a pu être transmis dans les temps, un possible report d'audience à la demande du prévenu[1027]. Enfin, la loi prévoit la possibilité, pour les parties, lors des débats de demander tous les actes qu'ils estiment utiles. Ces actes sont alors versés au dossier et soumis au contradictoire. Sans entrer dans les détails de la procédure, on ne peut nier que ce système renforce le principe du contradictoire et replace les parties au centre des débats ce qui a conduit une partie de la doctrine à y voir l'instauration d'un système de mise en état des procédures pénales.

L'évolution en faveur du droit au contradictoire dans la phase d'instruction semble plus marquée. Cette évolution s'observe notamment dans le droit accordé aux parties d'accéder au dossier dans sa totalité[1028] ou le droit pour les parties de formuler des observations ou déposer des requêtes à la clôture de l'instruction[1029]. Ce droit à être informé se concrétise également par l'accès au dossier d'instruction pour les parties. Plus précisément, une fois l'instruction ouverte, tout individu constitué partie civile et de manière général toutes les parties à la procédure peuvent obtenir copie des actes sans autorisation préalable[1030], qu'elles soient assistées ou non par avocat[1031]. En ce sens il faut rappeler la décision du Conseil constitutionnel du 16 septembre 2016 qui à l'occasion d'une question prioritaire de

[1022] Art. 393 et 394 du code de procédure pénale.
[1023] Rappelons qu'auparavant, le déferrement prenait la forme d'un énoncé des droits et d'une notification des faits sans réel échange entre le magistrat et la personne qui lui était présentée.
[1024] E. Daoud, A. Jacquin, L'effectivité du principe du contradictoire, *op. cit.*, p. 112.
[1025] Citation directe ou convocation par officier de police judiciaire.
[1026] Art. 388-4 du code de procédure pénale.
[1027] Art. 390-2 du code de procédure pénale.
[1028] Art. 114 du code de procédure pénale.
[1029] Art. 175 du code de procédure pénale.
[1030] Art. 114 du code de procédure pénale.
[1031] Cass., crim., 24 octobre 2018, *pourvoi* n° 17-82.816.

constitutionnalisé a jugé contraire à la Constitution l'article 197 de code de procédure pénale. Dans sa rédaction initiale, cet article réservait l'accès aux réquisitions du procureur de la République après notification de l'audience aux seules parties représentées[1032]. La Cour de cassation a rappelé que le principe vaut pour la partie civile qui doit être en mesure de prendre connaissance du dossier, affirmant que « les prescriptions de ce texte [article 197 du code de procédure pénale] ont pour objet de mettre en temps voulu les parties et leurs avocats en mesure de prendre connaissance du dossier, de produire leurs mémoires et d'être entendus à l'audience » ; rappelant « qu'il n'y est apporté aucune exception ni restriction à l'égard de la partie civile, lorsque l'audience porte sur la détention provisoire ou le contrôle judiciaire », la Cour de cassation a considéré que « la partie civile constituée au plus tard la veille de l'envoi d'avis d'audience par le procureur général, doit en être également rendue destinataire »[1033].

La Cour de cassation a précisé que le principe du contradictoire s'impose également à la chambre de l'instruction qui ne peut fonder sa décision sur un procès-verbal qui n'aurait pas été versé au dossier et soumis à débat contradictoire[1034].

En matière criminelle, l'article 279 du code de procédure pénale prévoit explicitement l'accès au dossier par la remise d'une copie des pièces aux accusés et parties civiles au stade du jugement. Ce principe s'applique également en cours d'audience. Si le versement de pièces nouvelles reste possible à ce stade, cela sous entend que ces dernières soient soumises au contradictoire et que toutes les parties aient le temps d'en prendre connaissance[1035].

347. Application du principe en matière civile – Ce droit à l'information résultant de l'application du contradictoire s'applique également en matière civile. L'article 15 du code de procédure civile dispose que « les parties doivent se faire connaître mutuellement en temps utile les moyens de fait sur lesquels elles fondent leurs prétentions, les éléments de preuve qu'elles produisent et les moyens de droit qu'elles invoquent, afin que chacune soit à même d'organiser sa défense ». On retrouve cette expression à l'article 135 qui permet au juge

[1032] Cons., const., 16 septembre 2016, n° 2016-566 QPC. De la même manière, la Cour européenne des droits de l'Homme avait condamné la France sur le fondement des droits de la défense du fait de l'accès limité au dossier prévu par les articles 114 et 19 du code de procédure pénale, entrainant à l'époque un revirement dans la jurisprudence de la Cour de cassation sur l'application des textes, excluant alors les dossiers dont une juridiction de jugement seraient saisis. (Cour E.D.H., 18 mars 19997, *Foucher contre France* n°22209/93).

[1033] Cass., crim., 27 mars 2019, *pourvoi* n°18-86.433. J. Chapelle, Rappel : le principe du contradictoire vaut également pour la partie civile, *AJ pénal*, 2019, p. 336.

[1034] Cass., crim., 6 novembre 2013, *pourvoi* n°13-85.618. En l'espèce, la chambre de l'instruction, allant contre les réquisitions du Parquet, ordonnait une mise sous contrôle judiciaire et fondait sa décision sur un procès-verbal de confrontation qui n'avait pas été versé au dossier et dont le mis en examen et le ministère public n'avait pas eu connaissance. La Cour de cassation rappelle donc la violation du principe du contradictoire.

[1035] Cass., crim., 9 ars 1994, *pourvoi* n°93-83.461.

d'écarter un document qui n'aurait pas été transmis en temps utile aux autres parties. Il appartient au juge de veiller à la mise en œuvre du contradictoire[1036] qui repose sur un échange spontané des pièces entre les parties[1037]. Ce dernier devant avoir lieu « en temps utile »[1038].

Le principe du contradictoire s'impose donc comme un garant du droit à l'information des parties à tout stade de la phase juridictionnelle. Son application soulève des interrogations plus spécifiques s'agissant de la nature personnelle de certaines données concernées.

Reprenant sa jurisprudence antérieure[1039], la Cour de cassation a rappelé que le juge ne peut pas écarter un moyen de preuve régulier qui aurait été soumis au débat contradictoire[1040]. La jurisprudence fait donc une application stricte du principe faisant du juge le garant de sa bonne application et affirmant un droit à être informé par la communication des pièces du dossier.

Malgré une application stricte et l'affirmation d'un droit à l'information dans le cadre de l'instance, le principe du contradictoire n'est pas absolu. Il existe des critères permettant de déroger au contradictoire, notamment s'agissant des données personnelles sensibles intervenant dans les expertises.

B. Le sort des données à caractère personnel dans l'application du principe du contradictoire dans le cadre d'expertises

348. Intérêt du sujet – Il ne s'agit pas là de revenir sur la question de l'accès aux données soumises au secret médical mais de s'interroger sur la question de l'application du principe du contradictoire lorsque le litige nécessite que soient versées au dossier des données sensibles et notamment des données médicales. L'importance accordée au principe du contradictoire ne fait pas de doute. Celui-ci peut primer lorsqu'il se retrouve confronté à des données protégées telles que des données médicales.

349. Les expertises judiciaires contradictoires sous réserve de respect de l'intimité – La question du traitement des données sensibles peut se poser notamment s'agissant des

[1036] Art. 16 du code de procédure civile.
[1037] Art. 132 du code de procédure civile.
[1038] Art. 15 du code de procédure civile.
[1039] Cass., mixte, 28 septembre 2012, *pourvoi* n°11-18.710.
[1040] Cass., civ. 2e, 7 septembre 2017, *pourvoi* n°16-15.531. Voir, E. De Leiris, O. Becuwe, N. Touati, N. Palle, Chronique de jurisprudence de la Cour de cassation, *Dalloz*, 2018, p. 757.

expertises. En matière d'expertise judiciaire civile[1041], le principe du contradictoire doit être respecté et ce même avant l'audience[1042]. Ainsi, par principe, les expertises sont réalisées en présence des parties. L'importance du respect du contradictoire a été affirmé par la jurisprudence. La Cour de cassation considère que les parties doivent être en mesure de discuter les données de l'expertise avant l'audience[1043]. En ce sens, les parties sont informées de la tenue d'une expertise et par principe sont conviées à y assister sous peine de nullité du rapport[1044]. La Cour européenne des droits de l'homme a affirmé le caractère contradictoire des mesures d'instruction confiées à un expert et ce notamment au vu du caractère déterminant que peuvent avoir de telles expertises dans le procès[1045]. Néanmoins, le respect du contradictoire ne doit pas porter atteinte à la vie privée et à l'intimité de la personne et peut justifier donc que les expertises ne soient pas réalisées en présence de toutes les parties.

Ce raisonnement trouve également à s'appliquer à la matière pénale[1046]. En l'espèce, la Cour de cassation a considéré qu'au regard du caractère intime de l'expertise celle-ci ne pouvait être réalisée en présence des parties.

L'intimité apparait donc comme une limite au principe du contradictoire[1047]. La notion de vie privée est large et le Conseil constitutionnel a reconnu qu'en découle l'inviolabilité du domicile et le secret des correspondances[1048]. De ce concept général, la jurisprudence est venue apporter des précisions permettant de mesurer la diversité des notions découlant du principe général. Le traitement des données à caractère personnel présentée par le Conseil constitutionnel comme « le reflet moderne de la personnalité »[1049] et sa protection ne se confond pas avec la notion de vie privée. On peut envisager que la révélation d'une information constitue une atteinte à la vie privée et de la même manière porte atteinte à la protection des données à caractère personnel. La notion de vie privée et de respect de l'intimité de celle-ci se veut plus large dans sa définition alors que la notion de données à

[1041] Art. 143 et s du code procédure civile.
[1042] A la différence de la matière pénale dans laquelle l'expertise elle –même n'est pas contradictoire, seuls ses résultats doivent être débattus par les différentes parties. (Cass., crim. 9 novembre 1972, *pourvoi* n°71-93.529).
[1043] Cass., civ. 1ère, 1er février 2012, *pourvoi* n°10-18.853.
[1044] Art. 160 du code de procédure civile.
[1045] Cour E.D.H., 18 mars 1997, *Mantovanelli c/ France*, 21497/93.
[1046] Cass, crim., 27 juin 2017, *pourvoi* n°17-80.411. C. Fleuriot, Expertise médicale et respect du contradictoire, *Dalloz actualité*, 17 juillet 2017. En l'espèce, le prévenu des faits de violences demandait l'annulation de l'expertise médicale réalisée sur la victime au motif qu'il n'y avait pas été convié et que le principe du contradictoire avait été violé.
[1047] A. Barrelier, L'intimité du corps humain comme limite au principe du contradictoire, *Gazette du palais*, 7 novembre 2017, n°38, p. 48. J.P. Vauthier, Expertise médicale et intimité de la victime : l'absence de l'auteur aux opérations d'expertise ne porte pas atteinte au principe du contradictoire, *RDS*, 2017, n°80, p.814-815.
[1048] Cons. const., 2004-492 DC, 2 mars 2004. Cons. const., 2014-420/421 QPC, 9 octobre 2014.
[1049] V. Mazeaud, La constitutionnalisation du droit au respect de la vie privée, *Nouveaux cahiers du Conseil constitutionnel*, n°48, juin 2015, p.7-20.

caractère personnel est définie plus strictement dans les textes mais renvoie finalement à un plus grand nombre d'informations[1050]. En effet, les textes encadrant le traitement des données à caractère personnel définissent strictement les données entrant dans leur champ d'application et fixent les règles relatives aux traitements en fonction de différents critères notamment leur finalité. En cela, il convient de dire que la protection des données à caractère personnel ne découle pas du droit au respect de la vie privée mais le complète et doit être interprété au regard de la vie privée. Quoi qu'il en soit, s'agissant du raisonnement de la Cour de cassation qui conduit à affirmer que l'intimité de la personne peut constituer une limite au contradictoire, ce même raisonnement semble transposable s'agissant de données personnelles. On peut imaginer qu'une expertise qui conduirait à révéler lors de sa réalisation des données à caractère personnel notamment sensibles puisse permette d'écarter le contradictoire au nom de la protection des données personnelles.

350. Le contradictoire dans le contentieux d'évaluation du préjudice suite à un accident du travail – La question du caractère contradictoire des expertises se pose également s'agissant des expertises relatives à l'évaluation du préjudice suite à un accident du travail ou à une maladie professionnelle. Il est admis que dans le contentieux de la contestation relative à l'état de santé, les rapports médicaux réalisés répondent au principe du contradictoire et sont transmises dans leur intégralité aux parties sans que puisse être opposé le secret médical[1051]. La Cour de cassation est venue préciser la portée de ces dispositions. Ainsi il ressort d'un arrêt du 8 mars 2001 qu'une fois l'expertise réalisée il appartient à l'organisme de sécurité sociale de la transmettre dans son intégralité à l'assuré sous peine de nullité de la procédure[1052].

Le contradictoire impose la communication des données entre les parties à l'instance, le principe de publicité quant à lui suppose une communication publique de certaines données et intéresse évidemment le sujet du traitement des données à caractère personnel.

[1050] Voir à ce sujet, E. Derieux, Vie privée et données personnelles – droit à la protection et « droit à l'oubli » face à la liberté d'expression, *Nouveaux cahiers du Conseil constitutionnel*, n°48, juin 2015, p.21-33.
[1051] Art. L142-6 du code de la sécurité sociale.
[1052] Cass., soc., 8 mars 2001, *pourvoi* n° . X. Prétot, Sécurité sociale, contentieux de la sécurité sociale, expertise médicale, communication du rapport d'expertise, principe du contradictoire, *Dalloz social*, 2001, p. 576.

§2. Les données diffusées par l'application du principe de publicité

351. Publicité et transparence – Si l'on observe la définition qui en est faite, la transparence renvoie au caractère de ce qui « laisse deviner » ou « qui ne dissimule pas »[1053]. L'idée d'une justice transparente est intimement liée au développement d'une société démocratique dans laquelle la justice est rendue pour le peuple. Ainsi, « la transparence parait se confondre avec la vérité, la clarté, la limpidité la pureté même » [1054] a pu écrire Jean-Denis Bredin. Cela renvoie au développement des lois dites de transparence ou de moralisation qui prônent de plus en plus la consécration d'un fonctionnement transparent des institutions avec en parallèle un recul des secrets. Cet affaiblissement des secrets trouve selon lui sa source dans le désir de vérité et est aussi la conséquence des développements technologiques de l'information[1055]. Il faut néanmoins distinguer le désir de vérité de tout un chacun et celui qui sert la justice. Ces évolutions sociétales, morales, et législatives ont amené certains à s'interroger sur le caractère absolu que pourrait avoir un droit à l'information au nom de cette transparence[1056]. Quoi qu'il en soit, face à l'affirmation d'une société transparente et d'un droit à l'information, les secrets restent les derniers remparts de protection des droits de la personne, de sa vie privée et de ses données à caractère personnel. Au niveau judiciaire, cette transparence se retrouve, notamment, au sein du principe procédural de publicité. La publicité de la justice est un principe fondamental du procès civil et pénal. Garantie procédurale, la publicité constitue une « exigence indispensable dans le procès pénal »[1057] et un « élément essentiel du procès équitable »[1058] découlant de l'article 6§1 de la Convention européenne des droits de l'homme. Ce principe est affirmé en droit international notamment au sein de l'article 10 de la Déclaration universelle des droits de l'homme[1059] ou à l'article 14 du Pacte international des droits civiques et politiques[1060]. Il repose sur l'idée générale selon laquelle, dans une société démocratique, la justice ne peut pas être rendue de manière cachée et secrète. De ce fait, le

[1053] Dictionnaire Larousse, 2013.
[1054] J.D. Bredin, « Secret, transparence et démocratie », *in* Pouvoirs, *revue française d'études constitutionnelles et politiques*, avril 2001, n°97p.5-15.
[1055] *Ibid*.
[1056] Voir, T. Massis, « La transparence et le secret, champ sociale débats de conscience », *in Etudes*, 2001/6, Tome 396, p.751-761.
[1057] S. Guinchard, J. Buisson, *Procédure pénale*, LexisNexis, 11e ed., 2018, p. 366 et s.
[1058] N. Fricero, S. Guinchard, *Droit et pratique de la procédure civile*, *op. cit*., chap. 212.
[1059] Art. 10 de la Déclaration universelle des droits de l'homme « toute personne a droit, en pleine égalité, à ce que sa cause soit entendue équitablement et publiquement par un tribunal indépendant et impartial... ».
[1060] Art. 14 du Pactes international des droits civiques et politiques « Toute personne a droit à ce que sa cause soit entendue équitablement et publiquement par un tribunal compétent, indépendant et impartial, établi par la loi, qui décidera soit du bien-fondé de toute accusation en matière pénale dirigée contre elle, soit des contestations sur ses droits et obligations de caractère civil ».

principe est celui d'une justice rendue publiquement garantissant ainsi un lien de confiance pour les justiciables. La publicité se révèle être un principe d'ordre public. L'article 592 du code de procédure pénale dispose que le non respect du principe de publicité des débats et du jugement entraine la nullité de la procédure. La Cour de cassation a rappelé qu'il s'agit « d'une règle d'ordre public à laquelle il ne peut être dérogé que dans les cas limitativement déterminés par la loi »[1061]. De la même manière, l'article 446 du code de procédure civile sanctionne par la nullité le non respect du principe. En termes de données à caractère personnel, le principe de publicité soulève des interrogations s'agissant de la diffusion de celles-ci. Contrairement au principe du contradictoire qui vise une communication des données aux parties, le principe de publicité a pour conséquence la diffusion publique des données. Le principe de publicité renvoie aux données du débat rendues publiques (A.) et aux données du jugement (B.).

A. Les données du débat rendues publiques

352. Publicité des débats – La publicité des débats soulève des interrogations en termes de diffusion des données à caractère personnel. Il convient de s'intéresser à la portée même du principe de publicité des débats (1°) pour s'interroger ensuite sur l'application faite du principe notamment s'agissant de la reproduction des débats dans la presse (2°).

1° La portée du principe de publicité des débats

353. Fondements du principe – Le principe de publicité des débats ou publicité de l'audience, renvoie à ce que certains qualifient de « recherche publique de la preuve »[1062] qui implique que l'audience nécessaire à la manifestation de la vérité soit faite publiquement. Trouvant son fondement dans l'intérêt général, le principe de publicité des procédures a été consacré en droit interne, et supranational. Dans l'arrêt du 8 décembre 1983 *Axen contre République fédérale d'Allemagne*, la Cour européen des droits de l'homme a considéré que la transparence de la justice permettait l'application de l'article 6§1 de la convention « préservant la confiance des justiciables dans l'institution judiciaire »[1063]. Aussi, dans l'arrêt du 24 novembre 1997, *Werner contre Autriche*, la Cour européenne expose que la publicité

[1061] Cass, crim., 9 novembre 2005, *pourvoi* n°04-87.471.
[1062] J. Pradel, *Procédure pénal*, Cujas, 2013, 17e ed., 848, p. 773.
[1063] Cour E.D.H., 8 décembre 1983, *Axen c/ République fédérale d'Allemagne*, 8273/78.

des débats protège « les justiciables contre une justice secrète échappant au contrôle du public »[1064]. Dans une importante décision, le Conseil d'Etat a affirmé que le principe de publicité permet aux justiciables de s'assurer que les décisions de justice sont rendues dans le respect du droit[1065]. Le principe de publicité renvoie donc à l'idée d'une justice équitable qui n'a de fait rien à cacher, ce qui s'inscrit parfaitement dans les principes d'une société démocratique[1066]. Si le principe repose sur l'idée d'un contrôle du peuple ou du moins d'un droit de regard sur l'application de la loi, il n'est pas pour autant un principe général et absolu et connait des exceptions[1067]. Affirmé sous l'égide des droits fondamentaux, la publicité des débats trouve des fondements en droit interne et une consécration jurisprudentielle.

Le principe est édicté à l'article 306 du code de procédure pénale s'agissant de la Cour d'assises, à l'article 400 en matière correctionnelle et à l'article 535 pour les procédures devant le tribunal de police. La chambre criminelle a qualifié le principe de publicité de principe essentiel de la procédure pénale[1068]. Le principe de publicité des débats a vocation à s'appliquer devant toutes les juridictions[1069]. La Cour de cassation a pu le rappeler à de nombreuses reprises précisant par exemple que le principe trouve à s'appliquer aux audiences relatives aux demandes de mise en liberté[1070] ou relatives à l'inexécution de travaux d'intérêt général[1071]. La mention de la publicité figure d'ailleurs sur les jugements. En matière civile, l'article 433 du code de procédure civile dispose que, sauf exception, les audiences sont publiques.

Le Conseil d'Etat a depuis longtemps reconnu l'importance du principe l'érigeant en principe général du droit[1072]. Le Conseil constitutionnel a reconnu l'importance du principe de publicité et cela ressort de différentes décisions. Il reconnait lui aussi le caractère général du principe en affirmant que la publicité doit s'appliquer aux audiences d'homologation de comparution sur reconnaissance préalable de culpabilité[1073], ou en matière d'audiences

[1064]Cour E.D.H., 24 novembre 1997, *Werner c/ Autriche*, 21835/93, n°27.
[1065] CE, 4 octobre 1974, *Dame David*, *req*. n°88930.
[1066] « la publicité des débats [est] une exigence démocratique essentielle », S. Guinchard, *Droit processuel*, *op. cit*., 582, p.1035.
[1067] *Supra* n°. En ce sens, dans l'arrêt 22 février 1984, *Sutter c/Suisse*, (req. no 8209/78, n° 30), la Cour européenne des droits de l'homme a considéré que le fait que l'absence de débats publics devant une instance jugeant en droit et non en fait (en l'espèce le tribunal militaire de cassation Suisse) ne violait pas le principe de publicité.
[1068] Cass., crim., 10 juillet 1074, *pourvoi* n°74-09.369.
[1069] Cour E.D.H., 20 janvier 2011, *Vernes c/ France*, req. n°30183/06.
[1070] Cass., crim., 22 avril 1970, *pourvoi* n°69-93.368.
[1071] Cass ., crim., 1er juin 1988, *pourvoi* n88-80.081.
[1072] CE, 4 octobre 1974, *Dame David*, *req*. n°88930.
[1073] Cons., const., 2 mars 2004, 2004-492 DC, §117, 118.

statuant sur une question prioritaire de constitutionnalité, le règlement intérieur prévoyant que les débats sont retransmis en direct dans une salle ouverte au public[1074].

354. Un principe relatif ? – Bien qu'affirmant le caractère général du principe, il ressort, toutefois, de la jurisprudence de la Cour européenne des droits de l'homme une certaine relativité dans l'application du principe liée à la possibilité laissé aux parties de renoncer à la publicité[1075].

2° La diffusion des données du débat par reproduction dans la presse

355. Les comptes-rendus de débats – Si le Conseil constitutionnel a pu estimer que l'atteinte faite à la liberté d'expression et de communication, du fait de l'interdiction de captation et d'enregistrement des audiences, est nécessaire et proportionnée, il précise que les dispositions de l'article 38 ter de la loi du 29 juillet 1881 n'interdisent pas au public présent à l'audience et notamment aux journalistes « de rendre compte des débats par tout autre moyen, y compris pendant leur déroulement »[1076]. Ainsi, le compte rendu rédigé, après prononcé public du jugement, sans partialité est couvert par l'immunité posée à l'article 41-3 de la loi du 29 juillet 1881 qui dispose que celui-ci ne peut donner lieu à une action en diffamation ou outrage[1077].

356. L'interdiction de captation, d'enregistrement et de diffusion des audiences conforme au principe de légalité des délits et des peines – L'article 38 ter de la loi du 29 juillet 1881 prohibe la captation et l'enregistrement de toute parole ou image d'une audience. Limitant les droits de la presse, l'article a fait l'objet d'une saisine du Conseil constitutionnel par la Cour de cassation par le biais d'une question prioritaire de constitutionalité. Il était notamment invoqué une atteinte à la liberté d'expression des journalistes et « le droit du public à recevoir des informations d'intérêt général ». A cette occasion, dans une décision rendue le 6 décembre 2019[1078], le Conseil constitutionnel a estimé que ces dispositions ont

[1074] Art. 8 du règlement intérieur du 4 février 2010.
[1075] Cour E.D.H. 23 juin 1981, *Le Compte, Van Leuven et De Meyere c/Belgique*, req. n°6878/75, 7238/5. Voir sur le sujet, N. Fricero, S. Guinchard, *Droit et pratique de la procédure civile, op. cit.*. 212. S. Guinchard, *Procès équitable, Garanties procédurales*, Répertoire de procédure civile mars 2017, 521.
[1076] Décision n°2019-817 QPC du 6 décembre 2019, cons. 9. M. Redon, *Tribunal correctionnel*, Répertoire de droit pénal et de procédure pénale, juin 2017 actualisation novembre 2020, 240. L'auteur fait notamment référence à la pratique du live-tweet qui semble autorisée au vu des dispositions de l'article 38 ter.
[1077] M. Redon, *Tribunal correctionnel*, Répertoire de droit pénal et de procédure pénale, *op. cit.*
[1078] Cons. Const., n°2019-817 QPC. J.M. Pastor, L'interdiction d'enregistrer les audiences ne méconnait pas la liberté de la presse, *AJDA*, 2019, p. 2521.

pour but de garantir la sérénité des débats et le droit au respect de la vie privée des parties et ce quand bien même seraient utilisés des moyens de captation modernes et discrets. Ensuite, le Conseil constitutionnel rappelle que cette interdiction ne s'oppose pas à ce que toute personne assiste à l'audience et s'il le souhaite en fasse un compte-rendu. En conséquence, le Conseil constitutionnel a jugé les dispositions nécessaires, adaptées et proportionnées au but recherché et qu'elles ne méconnaissent aucun des droits et libertés garantis par la Constitution. Ces dispositions visent donc outre le bon déroulement de l'audience, à garantir la vie privée et donc les données propres aux personnes et pour lesquelles la captation et la diffusion pourraient entrainer un préjudice pour les parties. Il s'agit donc bien ici par extension d'une protection accordée aux données rendues publiques lors de l'audience sous couvert de droit au respect de la vie privée.

357. L'interdiction de captation, d'enregistrement et de diffusion des audiences au nom de la bonne administration de la justice – Sur cette question la Cour européenne des droits de l'homme a eu à se prononcer sur la compatibilité entre l'interdiction posée à l'enregistrement et la diffusion des audiences et les dispositions de l'article 10 de la convention. Dans l'arrêt du 6 mai 2003 *P4 Radio Hele Norge ASA contre Norvège*, la Cour européenne a jugé conforme à la convention l'interdiction de retransmission[1079]. Rappelant que les Etats disposent d'une large marge d'appréciation dans la mise en œuvre des dispositions légales supra nationales, la Cour a également rappelé la nécessité de garantir la bonne administration de la justice. En l'espèce, elle a considéré que la diffusion en direct de l'audience était de nature à nuire au bon déroulement de celle-ci faisant peser des pressions sur les participants à l'audience. C'est donc au nom de la bonne administration de la justice que la Cour européenne admet une restriction à la liberté d'expression.

358. L'interdiction de captation, d'enregistrement et de diffusion des audiences au nom de la présomption d'innocence – La Cour européenne des droits de l'homme a parfois justifié l'interdiction par la nécessité de garantir les droits de personnalité de l'accusé et notamment la présomption d'innocence. C'est le cas dans l'arrêt du 21 septembre 2017 *Axel Springer SE et RTL Television GmbH contre Allemagne*, dans lequel la Cour européenne a considéré que le fait d'interdire la diffusion d'images sur lesquelles l'accusé est identifiable n'est pas disproportionné au nom de son droit à être présumé innocent. Certes, la Cour

[1079] Cour E.D.H., 6 mai 2003, *P4 Radio Hele Norge ASA c/ Norvège*, n°76682/01.

européenne des droits de l'homme fonde son raisonnement sur l'atteinte à la présomption d'innocence mais elle fait expressément référence au critère d'identificabilité afin de justifier l'interdiction. En adoptant une analyse très extensive de la décision et partant du postulat que le fondement de celle-ci reste la présomption d'innocence, la Cour européenne introduit dans son raisonnement la notion d'identificabilité sur laquelle repose la notion de donnée à caractère personnel, ce qui soulève la question de la restriction de la publicité sur le fondement de la nature des données en jeu. De manière générale, et peu importe le motif invoqué, la captation, l'enregistrement et la diffusion des audiences sont prohibés. Cette interdiction n'entache en rien la publicité des audiences mais se retrouve confrontée à la liberté d'expression et au droit de la presse. La Cour européenne des droits de l'homme affirme la prédominance des droits de la personnalité. Il serait, envisageable que soit invoqué la protection des données personnelles. Avec le développement récent d'un droit de la protection de ses données personnelles qui apparait plus large que le droit au respect de la vie privé, complémentaire de ce dernier mais pas concurrent, on peut envisager des restrictions sur ce fondement. Il faut toutefois mentionner que dans certains cas des exceptions peuvent être faites à cette prohibition. C'est le cas par exemple en matière d'archives. L'article L221-1 du code du patrimoine autorise l'enregistrement des audiences à des fins d'archives historiques.

Au-delà de la publicité des débats, le principe de publicité renvoie également à la publicité du jugement qui soulève des interrogations, pour certaines similaires, mais qui pose notamment la question de la publicité de la peine prononcée.

B. Les données du jugement rendues publiques

359. Fondements du principe – Le principe de publicité des jugements se retrouve aux articles 451 et suivants du code de procédure civile et à l'article 1016 concernant les arrêts de cassation. En matière pénale, ce principe est affirmé à l'article 400 du code de procédure pénale s'agissant des audiences correctionnelles, ces dispositions étant applicables devant le tribunal de police en vertu de l'article 535. Enfin il ressort de l'article 366 du code de procédure pénale que les arrêts de la Cour d'assises sont rendus publiquement. Le principe a vocation à s'appliquer à tous les contentieux quand bien même les débats auraient eu lieu en chambre du conseil ou à huis-clos. Le principe de publicité des jugements découle de l'article 6§1 du la Convention européenne des droits de l'homme. L'article 14 du PIDCP énonce que

« tout jugement rendu en matière pénale ou civile sera public ». Comme pour son application au cours des débats, la Cour européenne des droits de l'homme admet que le principe de publicité des jugements permet un contrôle de l'opinion sur les décisions rendues[1080]. Ce volet du principe de publicité a pu être présenté comme « le dernier bastion du principe de publicité de la justice »[1081].

360. Une publicité entendue largement – La Cour européenne des droits de l'homme semble faire une application moins stricte du principe s'agissant du prononcé du jugement. Ainsi, la Cour européenne considère que le principe de publicité du jugement peut prendre la forme soit d'un prononcé public soit d'un dépôt au greffe, l'accès au jugement étant suffisant[1082]. Aux côtés de la mise en œuvre de la publicité du jugement qui passe par le prononcé de la décision et la remise d'une copie aux parties, le courant actuel veut rendre ces décisions accessibles plus aisément au public faisant de la publication des décisions un pendant du principe de publicité traditionnel[1083]. La loi portant réforme pour la justice du 23 mars 2019[1084] va dans ce sens en prévoyant une diffusion des décisions de manière numérique et gratuite et un droit d'accès et d'obtention de copie du jugement pour les tiers. L'idée est de rendre les décisions de justice plus accessibles et plus disponibles. Cet accès suppose des mesures d'anonymisation ce que prévoit le décret du 29 juin 2020[1085].
Finalement, le principe de publicité a évolué en fonction des avancées technologiques. Il s'entend donc largement, puisque la mise à disposition suffit à remplir la condition de publicité et ce même par une mise à disposition numérique. Le sujet de la diffusion des données à caractère personnel dans le cadre d'une procédure judiciaire soulève également des interrogations s'agissant de l'accessibilité aux données en question.

Section 2 : Une approche extensive de la diffusion des données

361. Approche extensive – Au-delà des principes qui encadrent la publicité de la justice ou l'administration de la preuve et qui ont pour conséquence la diffusion des données de la

[1080] Cour E.D.H., 22 février 1984, *Sutter c/ Suisses*, 8209/78. F. Eudier, N. Gerbay, *Jugement*, Répertoire de procédure civile, octobre 2018 actualisation décembre 2020, 341.
[1081] P. Kayser, "Le principe de la publicité de la justice dans la procédure civile", *in* mélange Hébraud, *Dalloz*, 1981, p. 515.
[1082] Cour E.D.H. 8 décembre 1983, *Pretto c/Italie, req*. n°7984/77 et Cour E.D.H. 22 février 1984, *Sutter c/Suisse*, req. n° 8209/78.
[1083] Voir, V. Rivollier, L'open data des décisions de justice : pas tout, pas tout de suite, *Dalloz*, 2020, p.1626.
[1084] Loi n°2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la Justice.
[1085] V. *infra* n°412 s.

procédure, il convient de s'intéresser, par extension, aux données qui se trouvent nécessairement communiquées malgré le fait qu'elles bénéficient d'une protection particulière attachée au secret. Aussi, de manière plus générale, la diffusion des données a été repensée avec le recours de plus en plus marqué à la dématérialisation des procédures. Cette dématérialisation soulève des interrogations particulières s'agissant des données personnelles concernées. Ainsi, la question de la diffusion des données de procédure soulève par extension celle de la nécessaire communication de données protégées (§1.) et nécessité de s'interroger sur la diffusion facilitée par la dématérialisation des procédures (§2.).

§1. La nécessaire communication de données protégées

362. Communication nécessaire – Le secret qui entoure certaines données de la procédure peut céder dans certains cas strictement encadrés par la loi. Il s'agit donc d'observer dans quels cas et sous quelles conditions peut être autorisée la divulgation de données d'enquête et d'instruction (A.) ou de données couvertes par un autre secret professionnel (B.).

A. La divulgation de données d'enquête et d'instruction

363. Divulgation des données d'enquête et d'instruction – Bien que protégées, les données d'enquête ou d'instruction peuvent dans certains cas faire l'objet d'une divulgation. Cela est vrai lorsque la divulgation de donnes secrètes est justifiée sous couvert de protection de l'ordre public (1°), ou que leur communication est nécessaire dans une instance civile (2°).

1° La divulgation de données secrètes sous couvert de protection de l'ordre public

364. Protection de l'ordre public – Afin de préserver l'ordre public, il est admis que le procureur de la République puisse communiquer sur une affaire en cours d'enquête ou d'instruction. Cette éventualité est prévue à l'article 11 alinéa 3 du code de procédure pénale et vise à éviter la propagation d'informations fausses ou parcellaires susceptibles de créer un trouble à l'ordre public. Ces dispositions constituent les « fenêtres de publicité ». Cette possibilité a été rendue possible par la loi du 15 juin 2000 relative au renforcement de la présomption d'innocence et les droits des victimes. Toutefois, il ne peut communiquer au sujet des charges retenues ou de la culpabilité du prévenu. Le fait de communiquer sur un dossier en cours d'enquête ou d'instruction peut sembler opportun notamment dans le cas

d'affaire très médiatisées et éviter ainsi que la propagation de fausses informations viennent nuire à la procédure. Il s'agit, là encore, de ménager le juste équilibre entre le secret de l'enquête et l'information du public. Cette possibilité reste donc strictement encadrée. Le principe reste celui d'une enquête ou d'une instruction secrète et cette possibilité de communiquer certaines données vise justement à garantir son bon déroulement.

Au-delà, le procureur ne divulguant que certaines données permet d'assurer à la fois la présomption d'innocence des prévenus ou mis en cause et la protection de la vie privée des victimes par une information contrôlée et mesurée évitant que ne circulent certaines données inexactes ou faisant l'objet d'une interprétation erronée. De manière générale, le procureur de la République communique alors sur l'avancée de l'enquête et ses orientations sans pour autant révéler les données relatives aux parties ou aux charges retenues protégeant ainsi notamment les données à caractère personnel permettant d'identifier les protagonistes.

365. Communication sur des « éléments objectifs » - L'article 11 alinéa 3 vise des « éléments objectifs » de la procédure et ne doit donc pas faire référence à une quelconque appréciation des faits. Il semble donc que ces dispositions visent à protéger la présomption d'innocence et le bon déroulement de l'instruction. L'objectivité impose de faire une présentation factuelle de la situation et une présentation dans l'avancée théorique de la procédure, cela suppose de ne porter aucune appréciation sur les faits faisant l'objet de l'instruction. En tout état de cause, les dispositions précitées ne s'opposent pas à la communication de données permettant l'identification des suspects ou mis en cause. L'exercice semble toutefois empreint d'une certaine complexité tant la communication et le secret sont aux antipodes l'un de l'autre et semblent inconciliables[1086]. En effet le procureur de la République qui s'exprime sur l'instruction en cours doit s'assurer du respect d'autres principes au nombre desquels figurent la présomption d'innocence, le respect de la vie privée des individus, l'impartialité ou l'équité du procès[1087]. On comprend alors que ces propos doivent être mesurés. On peut mentionner également les dispositions déontologiques en vertu desquelles, « dans son expression publique, le magistrat fait preuve de mesure, afin de ne pas compromettre l'image d'impartialité de la justice indispensable à la confiance du public »[1088].

[1086] C. Guéry, *Instruction pénale*, Répertoire de droit pénal et de procédure pénale, *op. cit.*, 37.
[1087] J. Dallest, Le parquet et la communication ou les exigences de la modernité, *AJ Pénal*, 2018, 28.
[1088] Recueil des obligations déontologiques des magistrats.

2° La communication des données secrètes nécessaires dans une instance civile

366. Les données pénales dans le procès civil – Il s'agit ici de s'interroger sur la possible utilisation des données de la procédure pénale dans une instance civile (a°) et plus particulièrement sur l'utilisation des pièces d'une instruction en cours devant les juridictions civiles (b°).

a° La communication de données de procédures entre juridictions pénales et civiles

367. Communication entre juridictions – Il s'agit ici de s'interroger sur la possible utilisation des pièces du dossier pénal en cours devant une juridiction civile. Ses pièces peuvent, pour certaines, être nécessaire à l'indemnisation des victimes. S'agissant de l'indemnisation des victimes et de manière générale, l'article 706-6 du code de procédure pénale prévoit la possible communication de données du dossier pénal aux fins d'indemnisation des victimes. Ainsi, la commission d'indemnisation des victimes d'infractions[1089] peut notamment se faire communiquer une copie des procès-verbaux constatant l'infraction ou toute pièce du dossier pénal même si la procédure est en cours. De la même manière, le ministère public peut produire des pièces du dossier pénal lors d'une instance engagée par une association de consommateurs[1090] si elles sont nécessaires à la solution du litige. Suivant le même raisonnement, des pièces du dossier pénal peuvent être produites dans un litige relatif à l'indemnisation d'un préjudice lié à un accident du travail au profit du salarié, de l'employeur ou de la caisse de sécurité sociale[1091]. Enfin, à la suite d'un accident de la circulation, certaines pièces de dossier pénal peuvent être transmises aux compagnies d'assurance afin que celles-ci puissent mettre en œuvre le processus d'indemnisation relevant de l'assurance. De manière plus générale, se pose également la question de la possible communication en cours de procédure de données couvertes par un secret professionnel autre que le secret de l'enquête et de l'instruction.

[1089] Il s'agit d'une juridiction spécialisée composée de deux magistrats siégeant au sein de chaque tribunal judiciaire. Cette dernière au vu de la gravité des faits peut prononcer la réparation intégrale ou partielle.
[1090] Art. L. 421-8 du code de la consommation.
[1091] Art. L. 455-2 du code de la sécurité sociale.

b° La production par les parties dans une instance civile de données issues d'une instruction en cours

368. Problématiques – S'agissant du secret de l'instruction, la question peut se poser de la possibilité pour une partie à une instance civile de présenter des données issues du dossier pénal d'instruction. Si les parties à la procédure et les tiers ne sont par principe pas soumis au secret de l'instruction, car ne concurrent pas à cette dernière, peuvent-ils pour autant user librement des données couvertes par le secret ? A cette question, la Cour de cassation est venue apporter des précisions à l'occasion de différents contentieux[1092]. La transmission du dossier pénal soulève des interrogations légitimes notamment liées à la nature même des données qu'il contient tant sur les faits que sur la personnalité des auteurs présumés ou des victimes. Ces données peuvent donc pour certaines être qualifiées de données sensibles au sens de la loi informatique et libertés et du règlement européen sur la protection des données. Si la procédure pénale permet par nature de collecter et traiter de telles données en usant parfois de procédures exceptionnelles, qu'en est- il de l'instance civile et de la légitimité à présenter de telles données, les détournant ainsi de leur finalité pénale[1093] ?

369. Conditions d'accès au dossier d'instruction – Au-delà des questions d'interprétation de l'article 11 du code de procédure pénale[1094], et partant d'une lecture restrictive du texte[1095], la Cour de cassation affirme bien que les parties ne sont pas tenues par le secret de l'instruction. Toutefois, le législateur est venu étendre le droit d'accès au dossier d'instruction pour les parties et leur conseil en adoptant la loi du 30 décembre 1996[1096] qui a modifié le régime applicable en la matière[1097]. Désormais, l'article 114 du code de procédure pénale

[1092] Voir notamment le débat sur la qualité de tiers à l'instance du juge civil : C. Ribeyre, *La communication du dossier pénal*, *op. cit*., p.611 et suivantes.
L. Cadiet, E. Jeuland, *Droit judiciaire privé*, LGDJ, 11e ed., 2020, p. 353. Les auteurs rappellent que le juge n'est ni partie civile ni tiers à la procédure.
[1093] Voir à ce sujet, C. Ribeyre, *La communication du dossier pénal*, *op. cit*., p. 341. L'auteur s'est interrogé sur l'opportunité d'une communication du dossier pénal à des fins autres que pénales. Il rappelle que le principe reste celui d'une interdiction de communiquer et d'une protection du secret de la procédure pénale. Néanmoins des régimes d'exception existent devant nécessairement être prévus explicitement par la loi et strictement encadrés.
[1094] Voir notamment, E. Umberto Gout, Le sort des pièces de la procédure pénale devant le juge civil, *LPA*, 7 décembre 2018, n 245, p. 6.
[1095] L'article 11 dispose que le secret est opposable aux personnes qui concourent à l'enquête ou à l'instruction. *« Il n'y a pas de délit général de violation du secret de la procédure avant jugement, mais seulement un délit de violation du secret professionnel de la part des personnes qui, participant à la procédure, sont tenues au secret »*. J. Pradel, *Procédure pénale*, *op. cit.*, p. 459.
[1096] Loi n° 96-1235 du 30 décembre 1996 relative à la détention provisoire et aux perquisitions de nuit en matière de terrorisme.
[1097] Voir, C. Guéry, *Instruction pénale*, Répertoire de droit pénal et procédure pénale, *op. cit*., 471-479.

dispose qu'après la première comparution ou audition, les parties ou leurs avocats peuvent obtenir copie de tout ou partie du dossier. Ils doivent pour cela attester avoir pris connaissance des dispositions de l'article 114 et notamment son sixième alinéa qui dispose que **«** *Seules les copies des rapports d'expertise peuvent être communiquées par les parties ou leurs avocats à des tiers pour les besoins de la défense* ». L'avocat qui souhaite remettre une copie des pièces à son client doit en faire la demande auprès du juge d'instruction en application des alinéas sept à dix du même article. Dans sa demande, l'avocat mentionne la liste des pièces qu'il souhaite remettre à son client. Le juge d'instruction peut s'y opposer par ordonnance motivée notamment s'il estime qu'il existe un risque de pression sur la personne mise en examen, la victime ou les témoins. Cette décision peut faire l'objet d'un recours devant la chambre de l'instruction. Le non respect de cette procédure est constitutif d'un délit[1098]**.**

370. Production des pièces d'instruction au civil – Dans un arrêt du 23 novembre 2006, la cour de cassation affirme que *« la partie civile, qui n'est pas soumise au secret de l'instruction, tient de l'article 114 alinéa 6*^{e} *du code de procédure pénale la faculté de produire dans une instance civile, pour les besoins de sa défense, la copie d'un rapport d'expertise ordonnée par le juge d'instruction »*[**1099**]. Ainsi, la Cour de cassation admet dans un premier temps la possibilité de verser au dossier civil la copie du rapport d'expertise issu du dossier pénal en cours d'instruction. Toutefois, dans un arrêt du 30 juin 2016, la Cour de cassation énonce que *« **l**e secret de l'instruction n'est opposable ni aux parties civiles ni au ministère public ; que, dès lors, la cour d'appel a retenu, à bon droit, qu'il était loisible à ce dernier, partie jointe, de verser aux débats, pour être soumis à la discussion contradictoire des parties, tous documents ou renseignements de nature à contribuer à la solution du litige et qu'il pouvait autoriser les […] parties civiles, à communiquer des pièces extraites du dossier de l'information judiciaire alors en cours »*[1100]. En l'espèce, la Cour de cassation a retenu que les parties avaient été invitées par le conseiller de la mise en état à présenter au ministère public toute demande de production de pièces issues d'autres procédures. La Cour de cassation reprend ici le raisonnement qu'elle a eu lors de l'étude d'une question prioritaire

---

Avant la loi de 1996, l'avocat de la partie civile pouvait, à ses frais, obtenir copie du dossier pénal pour son « usage exclusif ». Il pouvait pour les besoins de la défense en donner connaissance à son client sans pour autant lui en fournir la copie, au nom du secret de l'instruction.

[1098] En vertu de l'article 114-1 du code de procédure pénale, le fait de délivrer le dossier à un tiers en méconnaissance des dispositions de l'article 114 est puni de 10000 euros d'amende.

[1099] Cass., civ. 2ème, 23 novembre 2006, *pourvoi* n°03-20490. V. Vigneau, sous la direction de T. Moussa, Cas particuliers d'intervention des sachants, *Droit de l'expertise*, Dalloz, 2016, chap. 212.

[1100] Cass., civ. 1ère, 30 juin 2016, *pourvois* n° 15-13755, 15-13904, 15-14145. N. Catelan, Arbitrage Tapie-Crédit Lyonnais : relaxe et relaps, *Dalloz actualité*, 26 juin 2019.

de constitutionnalité. Saisie d'une question portant sur la violation du principe d'égalité, des droits de la défense et du principe du contradictoire du fait de la possibilité offerte au procureur de transmettre des pièces du dossier d'instruction en cours lors d'une instance civile, la Cour de cassation a rejeté le renvoi au motif que la question n'était pas sérieuse et a rappelé que le procureur tient cette faculté de ses « missions spécifiques d'intérêt général »[1101]. Néanmoins, dans l'arrêt précité du 30 juin 2016, la Cour de cassation si elle réaffirme la possibilité pour le ministère public de verser au dossier toutes les pièces utiles issues d'autres procédures et en l'occurrence d'une instruction en cours, elle semble également affirmer la possibilité pour les autres parties civiles de se voir autoriser par le procureur à communiquer elles-mêmes ces pièces.

La question de l'accès aux pièces du dossier pénal en cours a fait l'objet d'éclaircissements notamment à la suite d'une question prioritaire de constitutionnalité à laquelle le Conseil constitutionnel a répondu le 16 décembre 2016[1102]. En effet, ce dernier avait jugé contraire à la Constitution les aliénas 3 et 4 de l'article 197 du code de procédure pénale relatifs à la mise à disposition du dossier d'instruction qui excluait les parties civiles non représentées par un avocat. Désormais, les dispositions de l'article 197 du code de procédure pénale prévoient la possibilité pour les parties non représentées de consulter le dossier d'instruction dans les mêmes conditions que les avocats. Néanmoins, l'article 114 alinéa 6 du code de procédure pénale précise bien que « Seules les copies des rapports d'expertise peuvent être communiquées par les parties ou leurs avocats à des tiers pour les besoins de la défense ». L'étude de la jurisprudence et notamment de l'arrêt du 30 juin 2016 au regard des dispositions légales sème le doute quant à la possibilité offerte aux parties d'user librement des pièces du dossier d'instruction en cours.

La diffusion des données de procédure soulève également la question de la possible communication des données couvertes par un secret professionnel.

B. La communication de données couvertes par un secret professionnel

371. Complexité entourant le secret professionnel – La recherche de la preuve se trouve bien souvent confrontée au secret professionnel. L'étude de la jurisprudence permet rapidement de comprendre la complexité qui entoure cette question dont l'issue dépend de différentes variables. Il convient de distinguer selon la nature du secret dont il est question.

[1101] Cass., crim., 30 septembre 2015, *pourvoi* n°15-90.014.
[1102] Cons. const., 16 septembre 2016, n°2016-566 QPC.

Aussi, l'approche sera différente en fonction du contentieux dans lequel les données couvertes par le secret sont invoquées. Enfin, les choses diffèrent également selon que les données sont communiquées directement par une partie à l'instance, suite à une demande au juge ou bien que leur production est ordonnée par l'autorité judiciaire. Par ailleurs, le statut du détenteur du secret a une importance dans l'application faite des textes selon qu'il est tiers à la procédure ou partie. Finalement, on comprend rapidement la complexité du système ce qui conduit certains auteurs à affirmer l'absence de théorie générale relative à cette question[1103]. En effet, l'étude de la jurisprudence fait davantage état d'une application au cas par cas des textes. Néanmoins, certaines décisions laissent apparaitre des lignes directrices qui pourraient constituer un semblant de théorisation en la matière.

S'agissant plus spécifiquement des données à caractère personnel, la question de la communication soulève celle de la communication de données couvertes par un secret. Ces données sont susceptibles d'être communiquées lors de l'instruction ou mise en état et lors de l'audience par les parties ou par des tiers, de leur propre fait ou sur demande du juge. La question est de savoir si le secret professionnel fait ou non obstacle à la communication de ces données et plus particulièrement si la nature de la donnée visée a une incidence en la matière. Pour reprendre une expression qui permet de bien cerner les enjeux, le secret professionnel renvoie à « une obligation de se taire et un droit au silence »[1104]. Il a pu être très justement rappelé que si la violation du secret professionnel se trouve incriminé par l'article 226-13 du code pénal, la soumission à ce secret relève d'autres textes qui viennent de fait « contrarier la loi pénale » [1105]. La levée potentielle du secret professionnel est donc liée à l'articulation de tous ses facteurs dont découle le choix de communiquer les données couvertes par le secret (1.) ou l'obligation de communiquer ces données (2.).

1° Le choix de communiquer des données couvertes par un secret

372. La liberté de révéler – Dans certains cas, l'individu en possession d'une information couverte par le secret dispose de la liberté de révéler ou non les données en sa possession. Cela renvoie en fait à plusieurs situations. Il peut s'agir pour un professionnel soumis au secret de choisir de révéler ou non une information dont il a eu connaissance à l'occasion de

[1103] B. Py, *Secret professionnel*, Répertoire de droit pénal et de procédure pénale, *op. cit.*. V. Peltier, *Révélation d'une information à caractère secret*, *op. cit.*

[1104] J.-L. Baudouin, *Secret professionnel et droit au secret dans le droit de la preuve*, LGDJ, 1965. B. Py, *Secret professionnel*, Répertoire de droit pénal et de procédure pénale, *op. cit.*, 78.

[1105] V. Peltier, *Révélation d'une information à caractère secret*, JurisClasseur pénal, *op. cit.*

l'exercice de sa mission, ce dernier disposant alors d'une « option de conscience » (a.), ou de la possibilité pour les parties non dépositaires du secret de produire des données couvertes par un secret (b°). Enfin il convient de s'interroger sur la communication par une partie dépositaire de données couvertes par le secret afin d'assurer sa défense (c°).

a° « L'option de conscience » du professionnel détenteur du secret

373. L'option de conscience – « L'option de conscience »[1106] vise la situation dans laquelle « *le professionnel [qui] est confronté à la délicate situation d'avoir à choisir entre respecter le secret et dénoncer une infraction* »[1107]. Il s'agit donc pour le dépositaire du secret d'un choix qui le conduit à soit communiquer l'information secrète soit se taire sans qu'aucune des deux possibilités ne puisse lui être reprochées sur le terrain de la violation du secret professionnel ou sur celui de l'article 434-1 du code pénal qui pose l'obligation de signaler un crime dont on a connaissance. Cette option de conscience vise tous les tiers à la procédure tenus par un secret qui disposent donc d'une « liberté de dénoncer »[1108]. Cette option intervient avant toute procédure puisqu'il s'agit pour le détenteur du secret de choisir en sa libre conscience de signaler les faits dont il a connaissance et qui sont susceptibles de constituer une infraction. Néanmoins cette donnée couverte par un secret demeure le point de départ d'une procédure il peut donc être intéressant d'étudier la question.

374. Option de conscience et secret médical – Cette option de conscience a pris une dimension particulière s'agissant des données couvertes par le secret médical et du choix pour le praticien de taire ou au contraire de divulguer ses données. Les faits d'atteintes sexuelles à caractère pédophile notamment ont conduit le législateur à inscrire explicitement dans les textes la possibilité pour le détenteur du secret de dénoncer les faits. Ces dispositions s'appliquent à tout détenteur d'une donnée couverte par le secret mais la nature même de l'incrimination fait du médecin une personne clé dans la dénonciation de tels crimes. Ainsi, l'article 226-14 du code pénal dispose que, le détenteur du secret relatif à des privations, sévices ou à des atteintes sexuelles infligés à un mineur ou à une personne vulnérable, peut dénoncer les faits auprès du procureur de la République, sans que la violation du secret ne lui

[1106] B. Py, Secret professionnel : le syndrome des assignats ?, *AJ pénal*, 2004, p. 133.
[1107] B. Py, *Secret professionnel*, Répertoire de droit pénal et de procédure pénale, *op. cit.*, 154.
[1108] C. Quennesson, *Mineur et secret*, A. Gouttenoire (dir.), thèse de doctorat, droit privé et sciences criminel, Université de Bordeaux, 2017, p. 282.

soit opposable[1109]. Il peut réaliser, sans l'accord de celui-ci, un signalement[1110]. En fonction de l'urgence de la situation et de sa gravité, le médecin[1111] peut soit transmettre une information préoccupante[1112] au Conseil départemental qui dispose d'une cellule spécifique au traitement de ces données, soit saisir directement le procureur de la République en faisant un signalement. L'information préoccupante concerne notamment les cas dans lesquels le professionnel est témoin de situation mettant en péril la santé ou la moralité du mineur ou lorsqu'il estime que son éducation et son développement sont compromis. Le but est de mettre l'accent sur une situation préoccupante et permettre une enquête sociale plus poussée. Néanmoins, si la situation révèle une menace imminente ou avérée le médecin doit saisir le procureur. Dans les deux cas, sa demande est accompagnée d'éléments médicaux. L'article 226-14 du code pénal précise que dans le cas de données médicales transmises lors d'un signalement, le médecin est délié du secret et ne peut être poursuivi ou sanctionné sur le plan disciplinaire, civil ou pénal. L'état de vulnérabilité permet la mise en œuvre d'un signalement s'agissant d'un majeur. Hors les cas de vulnérabilité, le médecin peut faire un signalement relatif à des sévices sur une personne majeure avec son consentement[1113]. Dans un premier temps, le médecin établit un certificat médical qui atteste des sévices et peut par la suite être cité comme témoin lors de l'audience. S'agissant du signalement concernant un adulte l'article 226-14 3° prévoit la possibilité pour le médecin de signaler des faits de violences exercées au sein du couple et ce sans que le consentement de l'intéressé ne soit forcément donné[1114]. En effet, le médecin doit « s'efforcer » d'obtenir cet accord mais lorsque cela est impossible notamment du fait d'une emprise exercée sur la personne, le médecin peut effectuer ce signalement sans l'accord de la personne en l'informant néanmoins de son intention d'effectuer cette procédure. Ces dispositions reprennent en réalité les dispositions déjà existantes qui permettent au professionnel de réaliser un signalement sans accord express de la personne s'agissant de personnes vulnérables. Les nouvelles dispositions reprennent donc ce principe l'appliquant au cas précis des violences intra conjugales. Cette mesure

[1109] La condition de vulnérabilité renvoie à l'incapacité pour la personne majeure de se protéger en raison de son âge, ou de son état physique ou psychique. A noter qu'initialement, le consentement était nécessaire pour un signalement relatif à un majeur vulnérable. Voir par exemple, Cass., crim., 27 avril 2011, *pourvoi* n°10-82.200. Dans cet arrêt la Cour de cassation a considéré que la Cour d'appel de pouvait pas condamner un médecin pour non dénonciation de mauvais traitements sans rechercher au préalable si ce dernier avait tenté d'obtenir le consentement de la victime afin de réaliser un signalement.

[1110] Art. 226-14 2° du code pénal.

[1111] Ou tout autre professionnel.

[1112] Dispositif prévu par la loi du 5 mars 2007 réformant la protection de l'enfance.

[1113] Il faut rappeler que le fait pour un patient de donner son consentement à la communication des données médicales ne délie pas le médecin de son obligation du secret.

[1114] Loi n°2020-936 du 30 juillet 2020 visant à protéger les victimes de violences conjugales.

soulève au-delà de son utilité en termes d'avancée législative des interrogations quant à sa portée. En effet, le conseil national de l'ordre des médecins semble soutenir ce dispositif à condition qu'il ne pose pas une obligation pour le médecin de signaler les faits mais bien qu'il rappelle l'option de conscience dont il dispose en la matière.

b° La production de correspondances privées

375. La production au cours de procédure de données issues de correspondances privées – Par principe les correspondances entre l'avocat et son client sont couvertes par le secret. Le secret des correspondances a pu être qualifié de « prolongement légitime du secret professionnel de l'avocat »[1115]. Ainsi, l'article 66-5 de la loi du 31 décembre 1971 dans sa rédaction issue de la loi du 11 février 2004 confirme le principe selon lequel toute correspondance entre l'avocat et son client est secrète. La jurisprudence est venue apporter quelques précisions relatives à la notion « de mention officielle » dans l'échange de correspondances entre avocats, qui constitue une exception au principe du secret. Dans un arrêt du 12 octobre 2016, la Cour de cassation a précisé que ne peuvent porter la mention « officielle » que les correspondances visées à l'article 3.2 du règlement intérieur national de la profession d'avocat[1116]. Ces dispositions visent les correspondances équivalant à un acte de procédure et celles « ne faisant référence à aucun écrit, propos ou éléments antérieurs confidentiels ». Le champ d'application de l'article 66-5 de la loi de 1971 semble donc plus restreint s'agissant des échanges de correspondances entre avocats. Toutefois, s'il appartient à l'avocat d'apposer la mention « officielle » sur les correspondances qu'il entend éventuellement produire en justice par la suite, la question demeure de savoir s'il l'apposition de cette mention se fait ou non avec le consentement du client[1117].

c. La communication par une partie dépositaire de données couvertes par le secret afin d'assurer sa défense

376. Communication par le dépositaire – Le dépositaire d'un secret peut-il communiquer les données qui lui sont confiées afin d'assurer se défense sans se voir opposer une violation

[1115] A. Andorno, Lettre officielle : l'habit ne fait pas le moine, *Dalloz*, 2017, 635.
[1116] Cass., civ. 1ère, 12 octobre 2016, *pourvoi* n°15-14.896. S. Grayot-Dirx, La mention « officielle » figurant sur une correspondance entre avocats ne suffit pas pour pouvoir la produire en justice, *JCP G*, n°45, 7 novembre 2016.
[1117] P. Bonfils, E. Gallardo, *Secret des correspondances*, Répertoire de droit pénal et de procédure pénale, avril 2018, actualisation juin 2018, 119. V. Peltier, Révélation *d'une information à caractère secret*, *op. cit*., 15.

du secret ? La Cour de cassation a très tôt apporté une réponse à cette question. Dès 1951, la Cour d'appel de Douai admet que le secret professionnel ne peut faire obstacle à la défense[1118]. S'agissant du secret qui lie le médecin à son patient, la Cour de cassation admet que ce dernier puisse révéler des données couvertes par le secret dans le but d'assurer sa défense. C'est ce qui ressort du célèbre arrêt du 20 décembre 1967[1119]. Ce même raisonnement a pu être appliqué au secret liant l'avocat à son client[1120] et au commissaire aux comptes[1121]. Finalement, la Cour de cassation admet depuis longtemps la levée du secret professionnel autorisant le dépositaire à révéler des données couvertes par ce secret dans le but d'assurer sa défense. Ce raisonnement tient à la protection des droits de la défense indépendamment du caractère absolu ou non attribué au secret. Si le secret liant le médecin ou le celui liant l'avocat ont pu être présentés comme recouvrant un caractère absolu, l'exercice des droits de la défense justifie que soit levé ledit secret professionnel. On peut dès lors considérer que ce raisonnement trouve à s'appliquer à tout dépositaire d'un secret professionnel, l'autorisant ainsi à communiquer s'il le souhaite des données couvertes par le secret.

Dans d'autres cas, malgré la nature des données couvertes par un secret, il existe une obligation de communiquer.

2° L'obligation de communiquer des données couvertes par un secret

377. Obligation de communiquer – Dans certains cas, le détenteur du secret ne dispose pas du droit de se taire ou de l'option lui permettent de choisir en conscience s'il divulgue la donnée ou non. Il peut en effet se trouver dans l'obligation de divulguer la donnée secrète en cas de péril pour la personne (a°), il peut être appelé à déposer en tant qu'expert (b°) ou dans certain cas, le dépositaire du secret peut être amené à révéler les données en tant que détenteur de données utiles à l'autorité judiciaire (c°). Enfin, le dépositaire d'un secret peut être amené à le révéler du fait de sa qualité de partie dans une procédure (d°).

a° L'obligation de divulguer la donnée secrète en cas de péril pour la personne

[1118] CA Douai, 26 octobre 1951,

[1119] Cass., crim., 20 décembre 1967, bull. crim. 338. Dans l'affaire dite du « roi des gitans », le médecin qui avait été contre son gré mêlé à une manœuvre frauduleuse l'ayant conduit à établir un faux certificat médical, peut pour assurer sa défense révéler des données couvertes par le secret médical.

[1120] Cass., crim., 29 mai 1989, bull. crim., 218.

[1121] Cass., com., 14 novembre 1995, bull. civ. IV., 262.

378. Péril pour la personne – Dans certains cas, le détenteur du secret n'a pas le choix et doit communiquer la donnée dont il a connaissance. L'inaction peut constituer le délit de non assistance à personne en péril[1122]. En effet l'article 223-6 du code pénal vise les cas où une personne a connaissance de faits portant atteinte à l'intégrité d'une personne et choisi de ne pas empêcher ces actes. Il s'agit donc là d'une obligation d'agir, l'article 223-6 du code pénal ne précisant pas les moyens de cette action. On peut donc envisager que dans certains cas le fait de dénoncer les faits constitue le seul moyen d'empêcher l'atteinte[1123]. Néanmoins, la portée de l'article 223-6 a pu soulever des interrogations. La notion de péril laissant place à diverses définitions. S'agissant des mineurs, l'organisation mondiale de la santé considère que « La maltraitance de l'enfant s'entend de toutes les formes de mauvais traitements physiques et/ ou affectifs, de sévices sexuels, de négligence ou de traitement négligent, ou d'exploitation commerciale ou autre, entraînant un préjudice réel ou potentiel pour la santé de l'enfant, sa survie, son développement ou sa dignité dans le contexte d'une relation de responsabilité, de confiance ou de pouvoir »[1124]. Elle vise donc les atteintes tant physiques que morales[1125] et il semble opportun de retenir cette définition.

Quoi qu'il en soit, l'article 223-6 du code pénal a une portée générale et ne tend pas à s'appliquer qu'aux mineurs posant ainsi une obligation pour tout détenteur d'un secret de révéler les données dont il a connaissance, autorisant ainsi la levée du secret. En pratique, il peut s'agir là encore souvent de données médicales permettant au professionnel le constat de tels sévices mais aussi de tout autre professionnel tenu au secret. Par exemple, l'avocat qui dans l'exercice de ses fonctions aurait connaissance de faits relatifs à de mauvais traitements exercés sur un mineur se trouve dans l'obligation de révéler ces faits si cette révélation constitue le seul moyen de mettre un terme à l'infraction, faute de quoi il commet l'infraction de non assistance à personne en péril[1126].

[1122] Art. 223-6 du code pénal.

[1123] Voir en ce sens, C. Quennesson, *Mineur et secret*, *op. cit*., p. 313 et s.

[1124] Définition posée par l'OMS voir https://solidarites-sante.gouv.fr/.

[1125] V. Malabat, *Droit pénal spécial*, Paris, Dalloz, Hypercours : cours et travaux dirigés, 7e éd., 2015, p. 248, n°461.

[1126] A. Gouttenoire, *Mineur*, Répertoire de procédure civile, juin 2015 actualisation décembre 2019, 265. L'auteure rappelle utilement que le professionnel soumis au secret professionnel n'est pas visé par les dispositions de des articles 434-1 et 434-3 du code pénal relatifs à la non dénonciation de crime ou de privations et mauvais traitements sur mineur.

b° Le détenteur du secret appelé à déposer en sa qualité d'expert

379. Le statut particulier du médecin expert – Il convient avant toute autre chose de s'intéresser au statut particulier du médecin expert. Ce professionnel de par ses fonctions est amené à recueillir des données d'ordre médical susceptibles par nature de constituer des données sensibles et qui par principe sont protégées par le secret professionnel. Néanmoins, le médecin expert désigné sur une liste établie par la Cour d'appel dispose d'un statut particulier. Lorsqu'il est appelé à déposer dans le cadre d'une procédure soit en versant un rapport au dossier soit en déposant à l'audience, ce dernier n'a pas le statut de témoin. En matière pénale en effet, l'article 168 du code de procédure pénale dispose que les experts sont appelés à exposer après avoir prêté serment « d'apporter leur concours à la justice en leur honneur et en leur conscience ». L'expert « n'est pas un confident de la personne expertisée mais un professionnel investi d'une mission de justice. À ce titre, il bénéficie de prérogatives comparables à celles du juge qui l'a désigné »[1127]. L'expert n'est pas soumis au secret médical lorsqu'il révèle des données médicales dont il a eu connaissance dans l'exercice de la mission pour laquelle il a été désigné[1128]. Aussi, afin de réaliser l'expertise, le médecin expert dispose de prérogatives et peut notamment demander à consulter le dossier médical de la personne sans que ne puisse lui être opposé le secret médical[1129].

380. L'exemple du secret médical et de l'expertise – La question du secret médical se pose, comme en matière de constatations, et plus encore, s'agissant des expertises faites sur ordonnance du juge. En effet, le recours aux expertises médicales tend nécessairement à intégrer aux dossiers des données de santé par nature sensibles. La question se pose du secret professionnel auquel se soumet l'expert en charge de l'expertise. Se pose également la question du secret médical qui peut être opposé à l'expert dans la réalisation de son analyse notamment lorsqu'il souhaite avoir accès au dossier médical de la personne concernée afin d'obtenir des renseignements utiles à sa propre analyse. Il peut s'agir d'expertises médicales, psychologiques ou psychiatriques. Ces expertises font l'objet d'un rapport remis au juge et versé au dossier. La question peut se poser tant en matière pénale que civile. L'expert réquisitionné pour réaliser l'expertise est soumis au secret professionnel s'agissant de toutes les données dont il aura connaissance au cours de son expertise. Aussi, la mission de l'expert

[1127] B. Py, *Secret professionnel*, Répertoire de droit pénal et de procédure pénale, *op. cit.*, 114.
[1128] Cass., crim., 1er décembre 1999, *pourvoi* n°99-82-067.
[1129] Cass., 1ère civ., 22 mai 2002, *pourvoi* n°00-16.305.

est limitée à la problématique posée dans la réquisition. En droit civil, l'expertise peut intervenir dès la mise en état ou dans le cadre de référés *in futurum*. Il a été précisé que l'expert ne peut dans son rapport révéler des informations dont il aurait eu connaissance en réalisant l'expertise qui n'entrent pas dans le champ de la réquisition[1130]. Le code de procédure pénale précise que l'expert doit se cantonner aux questions posées dans l'ordonnance[1131]. Les conclusions ne peuvent d'ailleurs pas être utilisées pour d'autres fins que celles pour lesquelles elles ont été ordonnées[1132]. La question se pose également du secret médical qui pourrait être opposé à l'expert dans l'exercice de sa mission. Le code de procédure civile précise que l'expert peut obtenir des informations auprès de toutes personnes[1133], et demander tout document lui semblant utile[1134], en recourant si nécessaire au juge. Lorsque l'expert souhaite consulter le dossier médical de la personne auprès de son médecin traitant, ce dernier peut, au nom du secret qui le lie, s'opposer à la transmission. Néanmoins, le juge pourra tirer les conséquences de ce refus. La Cour de cassation a précisé que le juge civil ne peut pas ordonner à l'expert la réalisation d'une mission qui méconnaitrait le secret professionnel[1135]. En matière pénale, le juge peut user de contrainte afin d'obtenir du médecin qu'il transmette le dossier à l'expert dans le cadre d'une enquête ou d'une information judiciaire. Il convient toutefois de préciser que si l'expert n'est pas soumis au secret s'agissant des données relatives à la mission ordonnée par le juge qui l'a saisi, tel n'est pas le cas s'agissant des autres données. En effet, en ce qui concerne les données qui ne relèvent pas de la mission pour laquelle l'expert a été désigné mais dont il a connaissance à l'occasion de celle-ci, ce dernier est soumis au secret professionnel.

c° Le dépositaire d'un secret appelé à révéler les données en tant que détenteur de données utiles à l'autorité judiciaire

381. Nécessités de la justice – Outre les cas de recours aux perquisitions et saisies[1136], l'officier de police judiciaire, le procureur de la République ou le juge d'instruction peuvent

[1130] Art. 244 du code de procédure civile.
[1131] Art. 158 du code de procédure pénale.
[1132] Art. 247 du code de procédure civile. *« L'avis du technicien dont la divulgation porterait atteinte à l'intimité de la vie privée ou à tout autre intérêt légitime ne peut être utilisé en dehors de l'instance si ce n'est sur autorisation du juge ou avec le consentement de la partie intéressée. »*
[1133] Art. 242 du code de procédure civile.
[1134] Art. 243 et Art. 275 du code de procédure civile.
[1135] Cass. civ. 1ère, 11 juin 2009, *pourvoi* n°08-12.742. En l'espèce, le juge avait missionné l'expert pour entendre tous les médecins qui avait put suivre la personne concernée sans l'autorisation de cette dernière.
[1136] V. *Supra* n°28 s.

dans le cadre d'une procédure requérir toute personne de fournir des informations ou documents utiles qu'ils ont en leur possession[1137]. Il s'agit ici de faire jouer le pouvoir de réquisition dont disposent les autorités judiciaires et qui leur permet, sauf « motifs légitimes » de demander la communication de données même couvertes par un secret professionnel. L'article 60-1 du code de procédure pénale prévoit la possibilité pour le procureur de la République ou l'officier de police judiciaire sous son contrôle, de requérir de toute personne, établissement ou administration toute information « y compris celles issues d'un système informatique ou d'un traitement de données nominatives ». Ces dispositions visent donc toutes données peu importe leur nature ou le secret qui les protège, mais aussi les données issues de traitement nominatifs et donc de données à caractère personnel. Le législateur entend donc prévoir explicitement l'accès aux données personnelles. Cela ressort des dispositions de la loi du 9 mars 2004 qui a doté les autorités judiciaires de nouvelles prérogatives d'enquête. Toutefois, il faut mentionner que lorsque la réquisition concerne un avocat, un organe de presse ou un médecin, leur accord est nécessaire[1138]. Néanmoins il convient de préciser qu'en cas de refus opposé par les professionnel, le juge peut recourir à la perquisition ou saisie des documents[1139]. Ces mécanismes se heurtent moins au secret professionnel ce qui conduit à dire que «cette protection n'est qu'une façade »[1140], puisque le secret professionnel ne peut pas faire obstacle aux perquisitions ou saisies.

Une inconnue demeure toutefois concernant l'étendue des « motifs légitimes » qui ne sont pas définis par les textes. Il semble donc délicat d'invoquer un motif légitime au refus de communiquer des données sans savoir par avance ce que ces motifs englobent.

Cette question de la portée du motif légitime trouve également à se poser en matière civile s'agissant des demandes de remise de pièces[1141]. Tout d'abord, l'article 10 du code civil pose l'obligation, sauf motif légitime, pour chacun d'apporter son concours à la justice. S'agissant des parties, l'article 11 du code de procédure civile vise « l'empêchement légitime ». En soi, le secret professionnel n'est pas par principe un motif légitime absolu, laissant aux juges le soin d'opérer une mise en balance des différents intérêts en jeu.

[1137] Art. 60-1 du code de procédure pénale.
[1138] Art. 56-1 à 56-5 du code de procédure pénale.
[1139] V. *supra* n°28 s.
[1140] V. Peltier, Révélation d'une information à caractère secret, *op. cit.*, 47.
[1141] J.H. Robert, *Administration judiciaire de la preuve*, JurisClasseur Procédure civile, Fasc. 700-12, 2 janvier 2017.

d° Le dépositaire appelé à s'exprimer du fait de sa qualité de partie

382. La levée du secret professionnel pour les parties – Peu importe le caractère absolu ou non du secret, il a été admis par la jurisprudence que lorsque le dépositaire est partie à la procédure il ne peut opposer le secret professionnel. Par exemple, la chambre commerciale de la Cour de cassation a jugé que l'établissement bancaire à qui l'on demandait la fourniture de données couvertes par le secret non en sa qualité de tiers confident mais en sa qualité de partie ne pouvait pas opposer le secret bancaire[1142]. Plus récemment, dans le cadre d'une demande de production forcée de pièces, la Cour de cassation a rappelé que la banque partie à la procédure ne peut opposer le secret professionnel comme empêchement légitime pour refuser de produire les documents demandés sur ce fondement estimant que *« le secret bancaire institué par l'article L. 511-33 du code monétaire et financier ne constitue pas un empêchement légitime au sens de l'article 145 du code de procédure civile lorsque la demande de communication de documents est dirigée contre l'établissement de crédit non en sa qualité de tiers confident mais en celle de partie au procès intenté contre lui en vue de rechercher son éventuelle responsabilité dans la réalisation de l'opération contestée »*[1143]. La Cour de cassation entend ici affirmer que le secret professionnel ne peut soustraire le détenteur à sa responsabilité. Néanmoins, il faut préciser que la Cour de cassation a, quelques années plus tôt, précisé que dans le cas où le contradicteur est non pas le client mais un tiers, le secret peut alors être opposé[1144]. Enfin, la Cour de cassation est venue préciser que dans le cas où c'est l'établissement bancaire qui intente une action en recouvrement, les débiteurs sont en droit d'obtenir les pièces qui justifient la créance réclamée quand bien même ces pièces sont couvertes par le secret[1145].

383. La levée du secret professionnel au nom du droit à la preuve – Certaines décisions prises sous l'influence de la jurisprudence européenne, prônent la levée du secret professionnel au nom du droit à la preuve[1146] Dans une décision du 16 juillet 2015, la Cour de justice de l'Union européenne a jugé qu'il convient de relativiser l'application et la protection

[1142] Cass., com., 19 juin 1990, *pourvoi* n° 88-19.618. Voir, G. Lardeux, Preuve, *Répertoire de droit civil*, *op. cit.*, 354.
[1143] Cass., com., 29 novembre 2017, *pourvoi* n°16-22.060. G. Lardeux, Preuve, *Répertoire de droit civil*, *op. cit.*, 357.
[1144] Cass., com., 10 février 2015, *pourvoi* n°13-44.779.
[1145] Cass., com., 16 décembre 2008, *pourvoi* n°07-19.777. G. Lardeux, Preuve, *Répertoire de droit civil*, *op. cit.*, 359.
[1146] A. Bergeaud, *Le droit à la preuve*, *op. cit.*

du secret au regard du droit à la preuve[1147]. Dans cette affaire, la victime d'une contrefaçon demandait la communication des données bancaires relatives à la transaction litigieuse. Elle s'est dans un premier temps vu opposer le secret bancaire. Le raisonnement de la Cour de justice est intéressant à plusieurs égards. Tout d'abord cette dernière confronte en l'espèce le droit au recours effectif garanti par l'article 47 de la charte de l'Union européenne et le droit à la protection des données à caractère personnel issu de l'article 8. De fait, la Cour de justice raisonne directement en termes de protection des données et non seulement en termes de secret professionnel. Aussi, cette dernière considère qu'en opposant le secret bancaire au requérant, les juges internes ont fait primer de manière excessive le secret sur le droit au recours effectif, supposant ainsi qu'il convient d'appliquer cette protection au regard de la nécessité de la preuve et donc du droit à la preuve. Le raisonnement adopté par la Cour de justice de l'Union européenne dans cette décision laisse supposer une portée générale. Ce même raisonnement a donc vocation à s'appliquer quel que soit le secret professionnel concerné ou quelles que soient les données personnelles en jeu.

Si le secret bancaire constitue un empêchement légitime en matière civile[1148], la chambre commerciale de la Cour de cassation a dans un arrêt du 15 mai 2019 affirmé qu'il convient de lever le secret professionnel si l'accès aux données est indispensable à l'exercice du droit à la preuve et que l'atteinte est proportionnée aux intérêts en jeu. Reprenant ainsi le raisonnement de la Cour de justice de l'Union européenne, la Cour de cassation considère que l'opportunité de communiquer ou non des données couvertes par un secret professionnel doit s'analyser au regard du droit à la preuve[1149]. La Cour de cassation reprend et complète le raisonnement d'un arrêt précédent en date du 4 juillet 2018 dans lequel il s'agissant d'une demande de production émanant de l'établissement bancaire[1150]. La Cour de cassation, dans l'arrêt précité du 15 mai 2019 vise directement l'article 511-33 du code monétaire et financier duquel découle l'empêchement légitime sans néanmoins y faire plus référence dans son développement. Aussi, la Cour de cassation rappelle que le secret bancaire est institué au bénéfice du client et non de l'établissement bancaire. De la même manière s'agissant du secret des affaires, la Cour de cassation dans un arrêt du 22 juin 2017 a estimé que dans le cadre d'une demande de production forcée de pièces, le secret des affaires ne peut pas être opposé si

[1147] Cour J.U.E., 16 juillet 2015, *Coty Germany GmbH*, aff. C580/13.
[1148] Voir par exemple, Cass., com., 13 juin 1995, *pourvoi* n°93-16.317. Cass., soc., 27 janvier 1999, *pourvoi* n°
[1149] Cass., com., 15 mai 2019, *pourvoi* n°18-10.491. En l'espèce, les requérants demandaient la communication de données bancaires sur le fondement de l'article 145 du cde de procédure civile et s'étaient vu opposer le secret professionnel. La Cour de cassation reprend ainsi les dispositions de l'arrêt du 5 avril 2012 qui consacre le droit à la preuve. Cass., civ. 1ère, 5 avril 2012, *pourvoi* n°11-14.177.
[1150] Cass., com., 4 juillet 2018, *pourvoi* n°17-10.158.

la pièce est indispensable à l'exercice du droit à la preuve et que l'atteinte est proportionnée[1151]. Là encore, la Cour de cassation reprend un raisonnement antérieur. En effet, dans un arrêt du 27 janvier 1999, cette dernière a jugé que le secret des affaires ne peut constituer un obstacle à l'application du l'article 145 du code de procédure civile dès lors qu'il y a un motif légitime de demander la production de la pièce et que celle-ci est nécessaire à la protection des droits des parties[1152]. Avec la consécration du droit à la preuve, la Cour de cassation semble s'appuyer sur celui-ci pour justifier parfois la levée du secret professionnel là où son raisonnement antérieur portait sur les droits de la défense. Toutefois, le droit à la preuve ne justifie pas nécessairement cette levée. La Cour de cassation l'a précisé s'agissant du secret notarial en affirmant que « le droit à la preuve découlant de l'article 6 de la Convention européenne des droits de l'Homme ne peut faire échec à l'intangibilité du secret professionnel »[1153].

Le raisonnement qui consiste pour la Cour de cassation à autoriser la levée du secret professionnel afin que puissent être garantis les droits de la défense se retrouve s'agissant du choix pour une partie de communiquer ou non des données couvertes par un secret[1154].

§2. La diffusion des données de procédure facilitée par la dématérialisation

384. Consécration d'un long processus – Le processus de dématérialisation des procédures a été engagé il y plusieurs années dans un but annoncé de simplification des échanges de données de la procédure entre les différents acteurs et de garantie de célérité. Ce phénomène s'inscrit dans l'évolution actuelle du système qui laisse de plus en plus de place au numérique[1155]. Pour autant, la dématérialisation des procédures n'est pas un phénomène récent. Devant les juridictions civiles, le décret du 28 décembre 2005 a posé les bases de la communication par voie électronique (CPVE) au sein des articles 748-1 et suivants du code de procédure civile[1156].

[1151] Cass., civ 1ère., 22 juin 2017, *pourvoi* n°15-27.845.
[1152] Cass., civ. 2ème., 7 janvier 1999, *pourvoi* n°95-21.934.
[1153] Cass., civ 1ère, 4 juin 2014, *pourvoi* n° 12-21.244.
[1154] V. *supra* n°
[1155] Avec par exemple la reconnaissance d'une valeur probante égale entre de la signature manuscrite et la signature électronique par la loi du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique.
Voir, A. Ouattara, *L'accès à la justice à l'épreuve du numérique*, dir. C. Tirvaudey, Mémoire, Droit, CRJFC, 30 septembre 2020, 102 p.
[1156] Décret n° 2005-1678 du 28 décembre 2005 relatif à la procédure civile, à certaines procédures d'exécution et à la procédure de changement de nom.

385. Les outils nécessaires à la dématérialisation des procédures – Ce processus de dématérialisation des procédures a nécessité de nombreux aménagements textuels et la création de nouveaux outils. Il a fallut adapter les textes de procédure aux nouveaux enjeux de procédures désormais numériques. Cette dématérialisation suppose que les acteurs de la justice disposent des moyens nécessaires à sa mise œuvre. Cela nécessité la création d'outils spécifiques et suffisamment sécurisés. Par ailleurs, la dématérialisation soulève des interrogations en termes de valeur probante des données numériques ce qui repose aussi sur la reconnaissance de la signature électronique ou sur la numérisation s'agissant des dossiers initialement papier. De la même manière, le recours à la visioconférence s'inscrit dans ce processus.

386. Les enjeux en termes de données – En termes de données traitées au cours des procédures, la dématérialisation soulève des interrogations spécifiques qui visent notamment la sécurité, l'accès ou encore la conservation.
La difficulté est d'appréhender un système de prime abord complexe car renvoyant à de nombreux dispositifs et outils qui supposent de comprendre un minimum l'outil informatique. Il convient donc de s'intéresser un premier lieu au cadre de cette dématérialisation pour pouvoir en cerner les problématiques en termes de traitement de données à caractère personnel. La mise en œuvre d'un traitement dématérialisé des données de procédure (A.) soulève des interrogations quant à la protection des données à caractère personnel dans ces procédures (B.).

A. La mise en œuvre d'un traitement dématérialisé des données de procédure

387. Finalités de la dématérialisation des procédures – Le monde judiciaire n'échappe pas au phénomène de dématérialisation qui touche tous les domaines. Annoncée comme garante d'une meilleure célérité des procédures avec en toile de fond un désengorgement des tribunaux et une meilleure information et transparence pour les justiciables, la dématérialisation de la justice est un mouvement de grande ampleur. Celui-ci est en œuvre depuis des années avec une accélération évidente ces dernières années.

388. Nécessaire création d'outils – La mise en œuvre de la dématérialisation des procédures judiciaires a nécessité la création de nouveaux outils permettant ce nouveau mode d'échange

de données et de communication entre acteurs des procédures. Ces nouveaux outils doivent être accompagnés de garanties quant à la sécurité des données traitées et à leur fiabilité.

389. Nécessaire adaptation du cadre juridique – La mise en œuvre de la dématérialisation des procédures judiciaires a conduit à repenser le cadre juridique et à l'adapter. Au-delà du fait qu'il a fallu encadrer les nouveaux outils et les nouveaux procédés nécessaires à sa mise en œuvre, la dématérialisation engagée il y a longtemps doit observer les normes relatives au traitement de données et notamment le règlement général sur la protection des données.
Ce mouvement de dématérialisation est progressif du fait de la nécessité de repenser le cadre juridique processuel afin de l'adapter à cette modernisation de la justice et du fait de la nécessité de créer les outils indispensables à celle-ci. Il convient d'observer les prémices de la dématérialisation des procédures judiciaires (1°) puis de s'intéresser à sa mise en œuvre en matière civile (2°) et pénale (3°).

1° Les prémices de la dématérialisation des procédures judiciaires

390. Dématérialisation – Le mouvement de dématérialisation des procédures judiciaires n'est pas récent mais il connait ces dernières années une forte accélération. Celui-ci repose à la fois sur l'adoption de textes mais aussi sur la signature de conventions-cadre entre le ministère de la justice et le conseil national des barreaux. La première convention-cadre est signée le 5 mai 2005 et définit le réseau privé virtuel des avocats (RPVA) comme service de communication entre avocats et juridictions[1157]. Suite à cela, un décret du 28 décembre 2005 est venu encadrer la communication par voie électronique (CPVE) en posant des dispositions communes à toutes les juridictions aux articles 748-1 et suivants du code procédure civile[1158]. Les dispositions prévoient notamment que le destinataire des communications par voie électronique doit avoir consenti expressément à l'usage de ce procédé[1159]. Le recours à la communication électronique doit garantir « la fiabilité de l'identification des parties à la communication électronique, l'intégrité des documents adressés, la sécurité et la confidentialité des échanges »[1160]. Aussi, il faut être en mesure de pouvoir dater l'émission et

[1157] Le RPVA a été mis en œuvre en décembre 2004 lors d'une Assemblée générale du CNB.
[1158] Décret n°2005-1678 du 28 décembre 2005 relatif à la procédure civile, à certaines procédures d'exécution et à la procédure de changement de nom.
[1159] Art. 748-2 du code de procédure civile.
[1160] Art. 748-6 du code de procédure civile.

la réception des documents[1161]. Un décret du 29 avril 2010 est en ce sens venu préciser que l'identification vaut signature d'un document numérique[1162]. Elle sera d'abord mise en œuvre dans certaines juridictions pilotes.

Une seconde convention-cadre en date du 28 septembre 2007 est venue étendre les recours à la communication électronique à la procédure pénale. Une troisième convention-cadre est venue, le 16 juin 2010 étendre le recours à la communication électronique notamment aux procédures civile en appel, cette dernière visant néanmoins les procédures civiles et pénales.

Sur les bases de la convention-cadre de 2010, a été signée celle du 24 juin 2016, qui adapte les dispositions en matière de communication électronique entre les juridictions ordinaires de premier et second degré et les avocats.

En 2017, a été lancé « le plan de transformation numérique de la justice » par le ministère de la justice visant à organiser le développement du numérique dans les échanges procéduraux et développer les outils nécessaires tout en prenant en compte des éventuelles difficultés rencontrées.

Le mouvement de dématérialisation concerne les procédures civiles et pénales, les conventions-cadre concluent, entre le ministre de la justice et le CNB, visent de manière générale les deux. Néanmoins, cette dématérialisation n'a été mise en œuvre de la même manière dans les deux contentieux ce qui nécessite une présentation distincte.

2° La mise en œuvre de la dématérialisation en matière civile

391. La communication par réseaux privés sécurités – La convention-cadre du 28 septembre 2007 prévoyait en matière civile la dématérialisation de la mise en état devant les tribunaux de grande instance.

Par anticipation, un arrêté du 25 septembre 2008 a permis la mise en œuvre de la CPVE devant certains tribunaux de grande instance[1163]. Ainsi, les dispositions des articles 748-1 et suivants ont été applicables s'agissant dans un premier temps des dépôts de requêtes, de la remise de copie d'assignations, de remise de conclusions ou pièces d'avocats ou de la copie des décisions rendues par le juge de mise en état.

[1161] *Ibid*.
[1162] Décret n°2010-434 du 29 avril 2010 relatif à la CPVE en procédure civile.
[1163] Arrêté du 25 septembre 2008 portant application anticipée devant les tribunaux de grande instance des dispositions relatives à la communication par voie électronique.

Par la suite, un décret du 9 décembre 2009[1164] est venu rendre obligatoire la communication dématérialisée en manière d'appel avec représentation obligatoire à peine d'irrecevabilité, sauf exception posée à l'article 930-2 du code de procédure civile[1165].
Un arrêté du 20 mai 2020 est venu abroger et remplacer les arrêtés dits « Cour d'appel » du 5 mai 2010 et du 30 mars 2011, permettant désormais le recours à la CPVE pour tous les actes autres que ceux prévus dans les anciens arrêtés sans que cela ne soit pour autant obligatoire.
Il faut également mentionner les dispositions de l'article 850 du code de procédure civile qui dispose qu' « à peine d'irrecevabilité relevée d'office, en matière de procédure écrite ordinaire et de procédure à jour fixe, les actes de procédure à l'exception de la requête mentionnée à l'article 840 sont remis à la juridiction par voie électronique »[1166], sauf cause étrangère[1167].

392. Le portail du justiciable – Des travaux relatifs à la réforme de modernisation de la justice est né le projet de création d'un portail unique du justiciable en matière civile dénommé Portalis. Ce dispositif vise sur le modèle de ce qui existe en matière pénale à dématérialiser la chaine civile dans sa globalité. Ce projet de grande ampleur s'est développé par étapes. Dans un premier temps le déploiement du site justice.fr vise à fournir aux justiciables une information qualitative et actualisée sur leurs droits et démarches[1168]. Ensuite la création des services d'accueil unique du justiciable (SAUJ) numériques vise à centraliser les procédures civiles, donnant accès aux greffiers habilités à toutes les procédures en cours sur le territoire national par le biais du réseau privé virtuel justice (RPVJ)[1169]. Le but étant pour ces personnels d'accueil des juridictions de pouvoir accéder aux données de procédure afin de renseigner les justiciables. Dans un premier temps, le décret du 3 mai 2019[1170] a

[1164] Décret n° 2009-1524 du 9 décembre 2009 relatif à la procédure d'appel avec représentation obligatoire en matière civile. Celui-ci est applicable depuis 2011.
[1165] Art. 930-1 du code de procédure civile. Ces dispositions ont été étendues aux procédures en droit social par décret du 20 mai 2016. Art. 930-2 du code de procédure civile « Les dispositions de l'article 930-1 ne sont pas applicables au défenseur syndical.
Les actes de procédure effectués par le défenseur syndical peuvent être établis sur support papier et remis au greffe ou lui être adressés par lettre recommandée avec demande d'avis de réception.
La déclaration d'appel est remise ou adressée au greffe en autant d'exemplaires qu'il y a de parties destinataires, plus deux. Le greffe constate la remise par la mention de sa date et le visa du greffier sur chaque exemplaire, dont l'un est immédiatement restitué. Lorsque la déclaration d'appel est faite par voie postale, le greffe enregistre l'acte à sa date et adresse un récépissé par lettre simple ».

[1166] L'article 840 du code de procédure civile vise la conciliation.
[1167] Art. 850 II. du code de procédure civile. Celui-ci reprend en partie les dispositions de l'article 796-1 du même code, abrogé par le décret du 11 décembre 2019 qui prévoyait de manière générale le recours à la CPVE pour tous les actes.
[1168] Le site est effectif depuis 2016.
[1169] Loi n° 2016-1547 du 18 novembre 2016 de modernisation de la justice du XXIe siècle.
[1170] Décret n°2019-402 du 3 mai 2019, portant diverses mesures relatives à la communication électronique en matière civile et à la notification des actes à l'étranger.

ouvert la possibilité de recevoir les convocations et avis des juridictions via le portail à condition d'y consentir. Ensuite, l'arrêté du 18 février 2020[1171] marquent une nouvelle étape dans le déploiement du portail en permettant d'adresser les requêtes en ligne s'agissant des procédures devant le juge de tutelles dans un premier temps et le projet d'une extension à toutes les procédures[1172].

Cette nouvelle fonctionnalité du portail n'est pas sans soulever des interrogations quant à la sécurité des données traitées. S'agissant du traitement de données à caractère personnel par le biais de ce portail, l'arrêté du 28 mai 2019[1173] est venu apporter de précisions. Il ressort de ces dispositions que peuvent être enregistrées dans le fichier les données à caractère personnel relatives au consentement de l'utilisateur, l'adresse électronique du justiciable, son numéro de téléphone mobile, le numéro d'affaire Portalis, la clé de fédération générée par FranceConnect, le nom de la juridiction en charge de l'affaire, la date de sa saisine, la nature de l'affaire, les données identifiantes relatives aux parties et à leurs représentants, le statut de l'affaire et les informations relatives aux audiences[1174]. Ne peuvent accéder aux données que le justiciable et les personnels du greffe habilités par leur directeur de greffe[1175]. Aussi, comme pour tout traitement de données à caractère personnel et suivant la ligne de conduite fixée par le règlement européen sur la protection des données, le justiciable dispose d'un droit d'accès et de rectification des données ainsi que d'opposition au traitement[1176]. Ce droit s'exerce par saisine du ministère de la Justice. Ce nouveau dispositif semble de prime abord reprendre les grands principes posés au niveau européen s'agissant de la protection des données mais demeure néanmoins complexe à appréhender de par notamment la multitude de texte adoptés en la matière[1177].

[1171] Arrêté du 18 février 2020, modifiant l'arrêté du 28 mai 2019 autorisant la mise en œuvre d'un traitement automatisé de données à caractère personnel dénommé « Portail du justiciable » (suivi en ligne par le justiciable de l'état d'avancement de son affaire judiciaire).

[1172] Voir, C. Bléry, J.P. Teboul, Dématérialisation des procédures : saisine d'une juridiction par le portail du justiciable, *Dalloz actualité*, 5 mars 2020.

[1173] Arrêté du 28 mai 2019 autorisant la mise en œuvre d'un traitement automatisé de données à caractère personnel dénommé « portail du justiciable », JORF n°0130, 6 juin 2019.

[1174] Arrêté du 28 mai 2019 autorisant la mise en œuvre d'un traitement automatisé de données à caractère personnel dénommé « portail du justiciable », article 2.

[1175] Arrêté du 28 mai 2019 autorisant la mise en œuvre d'un traitement automatisé de données à caractère personnel dénommé « portail du justiciable », article3.

[1176] Arrêté du 28 mai 2019 autorisant la mise en œuvre d'un traitement automatisé de données à caractère personnel dénommé « portail du justiciable », article 5.

[1177] Voir en ce sens, C. Bléry, J.P. Teboul, Dématérialisation des procédures : saisine d'une juridiction par le portail des justiciables, *Dalloz actualité*, 5 mars 2020. Les auteurs soulèvent notamment la confusion attachée à l'usage des termes : plateforme, traitement automatisé et site internet utilisés selon eux de manière propice à confusion.

3° La mise en œuvre de la dématérialisation en matière pénale

393. La dématérialisation des procédures pénales – En matière pénale, cette évolution a débuté avec la création du logiciel de chaine pénale « Cassiopée » qui a mis un terme aux fiches papier de suivi des procédures.

Aussi, un arrêté du 16 janvier 2008, a mis en œuvre la numérisation des procédures pénales papiers par le traitement de « numérisation des procédure pénales » (NPP)[1178] qui sont alors stockés sur un serveur sécurisé. Initialement, faisaient l'objet d'une numérisation, les procédures criminelles ou certaines affaires complexes[1179]. Dans la lancée de ce qui a été engagé en 2008, est née l'idée d'une dématérialisation totale des procédures pénales. L'objectif annoncé est là aussi celui d'une meilleure efficacité du système judiciaire par une dématérialisation des échanges entre les différents acteurs de la procédure. Ainsi l'échange de données de manière dématérialisée serait plus rapide permettant ainsi une meilleure collaboration entre les acteurs, notamment entre les juridictions et les enquêteurs.

Le projet de mise en œuvre de la procédure pénale numérique (PPN) est présenté comme permettant de garantir une meilleure force probante des pièces de procédure, puisque le dossier numérique sera plus protégé car accessible seulement par un accès sécurisé. En outre, il est avancé le fait que la version numérique devenant la version initiale, ne se pose plus la question des copies conformes ou non, l'accès au dossier numérique donnant accès à la pièce originale.

394. La création du « dossier pénal numérique » - Dans cette optique a été créé le « dossier pénal numérique » par décret du 23 juin 2020. Ce dernier abroge et englobe les dispositions relatives au traitement NPP. Sur ce nouveau traitement, la CNIL a formulé quelques observations dans son avis portant sur le projet de décret en date du 12 mars 2020[1180]. La Commission suggère que soit mentionnée la qualité des personnes qui assistent les magistrats et qui de fait ont accès aux données. Aussi, la Commission soulève que si le dossier pénal

[1178] Dans une délibération du novembre 2010, la CNIL a considéré que le traitement visait à faciliter l'accès des parties aux données de la procédure et favorisait l'exercice des droits de la défense et le débat contradictoire. En cela, sa finalité était légitime. Aussi, les données étant conservées jusqu'à l'exécution des peines, la durée de conservation était justifiée. Enfin, l'accès par authentification au traitement et la diffusion par réseaux privés (RPVA/RPVJ) sécurisé garantissait selon elle la sécurité des données. (délibération 2010-411).

[1179] Voir, S. Chassard, Numérisation et communication électronique en matière pénale : quels enjeux, quels apports, quelles contraintes, quelles implications dans la procédure sur le quotidien d'un magistrat du Parquet ? *AJ pénal*, 2014, p.156.

[1180] Délibération CNIL n°2020-036 du 12 mars 2020 portant avis sur un projet de décret portant création d'un traitement automatisé de données à caractère personnel dénommé « dossier pénal numérique ».

numérique peut être mis en relation avec d'autres traitements de données, cela ne peut avoir pour conséquence d'élargir le nombre de personnes ayant accès au dossier. En outre, la Commission avait estimé dans son avis que les garanties en termes de sécurité n'étaient pas suffisantes. Comme cela a été soulevée par le passé, l'interconnexion et la mise en relation des fichiers peut constituer une source d'erreurs et d'insécurité pour les données. Néanmoins, le dossier pénal numérique n'est pas interconnecté avec d'autres traitements tels que Cassiopée, et il n'y a pas d'échanges de données avec d'autres fichiers tels que le TAJ, le FEAD ou la FNAEG. S'agissant des données sensibles, la CNIL rappelle les dispositions de l'article 88 de la loi informatique et libertés du 6 janvier 1978 en vertu duquel n'est autorisé le traitement de telles données qu'en cas de « nécessité absolue » et sous réserves de « garanties appropriées pour les droits et libertés de la personne concernée ». Concernant l'accès au dossier, la CNIL a rappelé la nécessité de répondre aux exigences posées dans sa délibération du 19 janvier 2017 s'agissant des mots de passe et rappelle que l'accès doit être nominatif et individuel. Le décret du 23 juin 2020 portant création du dossier pénal numérique prévoit, s'agissant de la diffusion des données, que peuvent accéder aux données les magistrats, les greffiers ainsi que les délégués du procureur ou les avocats en fonction de ce qui est nécessaire à l'exercice de leurs fonctions[1181]. Dans une moindre mesure peuvent accéder à tout ou partie du dossier les parties, leurs avocats, toutes personnes concourant à la procédure au sens de l'article 11 du code de procédure pénale et toute administration, établissement, autorité, ou personne publique ou privée autorisés[1182]. Certains et notamment des associations dénoncent une collecte « inutile et disproportionnée »[1183] de données portant notamment sur l'orientation sexuelle des personnes dont les victimes et témoins. Ce stockage de données concerne les victimes, mis en causes, témoins, les personnes poursuivies, condamnées ou faisant l'objet d'une enquête. Au delà de la diversité des personnes susceptibles de voir leurs données personnelles stockées dans le dossier, ces données en questions peuvent être diverses. En effet, le dossier pénal numérique contient des données relatives à l'identité des individus, à leur situation familiale, administrative, patrimoniale ou biométrique par exemple. Toutefois, dans l'avis rendu, la Commission nationale de l'informatique et des libertés ne semble pour sa part pas avoir émis de réserves quant à la nature des données traitées et a considéré que les

[1181] Art. R249-13 I. du code de procédure pénale.
[1182] Art. R249-13 II. du code de procédure pénale.
[1183] Association de lutte contre les discriminations liées au sexe, au genre et à l'orientation sexuelle (Mousse), « Dossier pénal numérique : recours devant le Conseil d'Etat contre la collecte des données liées à l'orientation sexuelle », *in Assomousse.org* [en ligne], publié le 6 juillet 2020, consulté le 27 septembre 2020.

données enregistrées étaient « adéquates, pertinentes et non excessives »[1184]. La Commission a toutefois rappelé le caractère nécessaire de tout traitement de données sensibles, et visant particulièrement les données d'enquête ou d'instruction, elle rappelle l'impératif de respect des règles édictées par la loi. La dématérialisation des procédures soulève la question de la communication des données faisant l'objet d'une protection particulière et plus particulièrement des données couvertes par le secret de l'enquête ou de l'instruction, et des données judiciaires.

395. Les réseaux privés virtuels – Il faut aussi rappeler que le RPVA et le RPVJ ont vocation à être utilisée en matière pénale également. La Cour de cassation l'a d'ailleurs clairement rappelé dans un arrêt du 11 décembre 2013 précisant que « depuis le 7 janvier 2013, l'avenant du 25 juin 2012 à la convention conclue entre le tribunal de grande instance et l'ordre des avocats de Paris le 28 janvier 2009, pris en application de l'article D. 591 du code de procédure pénale, permet aux avocats de ce barreau de transmettre, à partir de leur adresse électronique sécurisée, par un moyen de télécommunication, à l'adresse électronique de ce tribunal les demandes d'actes prévues par l'article 82-1 de ce code, selon les modalités prévues à ladite convention »[1185].

Le développement du mouvement de dématérialisation des procédures soulèvent des interrogations légitimes en termes de protection de données notamment au vu de quantité des données visées par tous les traitements nécessaires à sa mise en œuvre.

B. La protection des données à caractère personnel dans une procédure dématérialisée

396. Traitement massif de données sensibles – Les outils mis en œuvre afin de basculer dans une procédure judiciaire dématérialisée reposent sur des traitements de données visant la collecte, le rapprochement, la conservation et l'échange de celles-ci. Ces données de procédure sont potentiellement des données sensibles ou pour certaines protégées. Partant de la protection des données prévue par les textes (1°), le recours à des outils sécurisés s'avère nécessaire (2°) et amène à s'interroger sur le traitement dématérialisé des données protégées (3°).

[1184] Délibération CNIL n°2020-036 du 12 mars 2020 portant avis sur un projet de décret portant création d'un traitement automatisé de données à caractère personnel dénommé « dossier pénal numérique », 26.
[1185] Cass,, crim., 11 décembre 2013, *pourvoi* n° 13-84.319.

1° La protection des données prévue par les textes

397. La protection des données prévue par les textes - Le règlement général sur la protection des données (RGPD) qui a vocation à responsabiliser les acteurs de traitements de données personnelles insiste sur le fait que tout traitement doit se faire sous le contrôle d'un responsable. De manière générale, il appartient au responsable du traitement de veiller à la sécurité des données. Ce dernier est « tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès »[1186]. S'agissant des données judiciaires liées aux condamnations ou aux infractions, ce responsable ne peut être que l'autorité publique[1187]. Dans le but d'assurer une protection renforcée des données à caractère personnel, le règlement européen et la loi informatique et liberté dans sa nouvelle rédaction ont édicté des obligations qui incombent aux responsables du traitement. Toutefois, les traitements relatifs au fonctionnement de la justice font l'objet d'un régime particulier puisque certaines des règles posées et notamment des obligations incombant au responsable du traitement ne trouvent pas à s'appliquer. L'article 107 de la loi informatique et libertés précise que les droits des personnes visées par le traitement peuvent être restreints notamment lorsqu'il s'agit de traitements liés à des enquêtes ou à des procédures judiciaires. L'article précise ainsi que ces droits ne peuvent « nuire à la prévention ou à la détection d'infractions pénales, aux enquêtes ou aux poursuites en la matière ou à l'exécution de sanctions pénales »[1188]. Aussi, il ressort de l'article 111 de la loi informatique et libertés que certaines des obligations qui incombent au responsable du traitement ne s'appliquent pas s'agissant des données à caractère personnel contenues dans une décision judiciaire ou dans un dossier pénal de procédure. Dans ces cas, l'accès, la rectification des données ou l'effacement est régi par le code de procédure. La CNIL, qui s'est vue dotée de pouvoirs de sanction a posteriori, dispose désormais de nouveaux moyens d'action allant du simple rappel à l'ordre, ou injonction de mise en conformité à l'amende administrative ou au prononcé de l'interruption du traitement. Toutefois, s'agissant des traitements intéressants la sureté de l'Etat ou mis en œuvre pour le compte de l'Etat, la Commission ne peut prononcer qu'un rappel à l'ordre ou une injonction

[1186] Art. 121 de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la l'ordonnance du 12 décembre 2018.
[1187] Art. 10 du règlement général sur la protection des données du 23 mai 2018.
[1188] Art. 107 de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la l'ordonnance du 12 décembre 2018.

de mise en conformité non assortie d'astreinte[1189]. Finalement, la CNIL ne dispose que de peu de moyens d'action s'agissant des données traitées en matière judiciaire par les autorités compétentes. La loi renvoie en la matière aux dispositions du code de procédure pénale et du code pénal et notamment aux articles 226-16 à 226-24 du code pénal qui incriminent toute atteinte aux droits de la personne résultant de fichiers ou de traitement informatiques. En l'état actuel, la législation interne vise en la matière une responsabilité personnelle sur le fondement notamment d'une atteinte à la vie privée. Le règlement européen prône quant à lui un droit à la protection des données personnelles.

2° Le recours nécessaire à des outils sécurisés

398. Brefs rappels – La complexité du système mérite un bref rappel quant à l'étendue des outils nécessaires à la mise en œuvre de la dématérialisation des procédures. La dématérialisation nécessite que les procédures soient numérisées ou sous format nativement numérique. Cela nécessite pour les premières le recours à ces traitements de numérisation qui sous-entendent ensuite un stockage sécurisé des données. Les procédures sont enregistrées sous des applications qui permettent de suivre les avancées de celles-ci tout en alimentant et mettant à jour en permanence. Il s'agit de Cassiopée pour la chaine pénale et de WINCI pour la chaine civile. La communication entre juridictions et cabinets d'avocats a nécessité la création de modules tels que COMCI en matière civile. Les avocats quant à eux utilisent le « e-barreau » afin de communiquer avec les juridictions. Il s'agit d'un portail sécurisé qui permet d'échanger avec les greffes sur les affaires en cours et consulter l'avancée du dossier. Afin d'échanger des pièces et données, les juridictions utilisent les RPVJ et les avocats le RPVA qui sont des réseaux sécurisés.

399. La création de réseaux privés virtuels – La dématérialisation passe par le développement de réseaux privés sécurisés. Il s'agit par exemple du réseau privé virtuel justice (RPVJ) ou du réseau privé virtuel des avocats (RPVA). Ces réseaux sont sécurisés et accessible par le biais d'interface sécurisées. Ces réseaux privés permettent l'échange de données sécurisé entre professionnels puisqu'il nécessite un haut degré d'authentification.

[1189] Art. 20 et art. 21 de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la l'ordonnance du 12 décembre 2018.

400. La création d'une plateforme d'échange via les réseaux privés – Aux côtés de ces réseaux privés a été crée une plateforme d'échange. Par deux arrêtés du 24 octobre 2019 ont été créés deux fichiers de traitement automatisés dénommés PLINE et PLEX[1190] et fixés les modalités d'échange par le biais de ces plateforme[1191]. Il s'agit de deux plateformes d'échange pour l'une interne au ministère de la justice (PLINE) et pour l'autre permettant des échanges externes (PLEX) accessibles via les réseaux privés (RPVJ). L'accès se fait par le biais d'identifiants strictement personnels[1192] et les données stockées font l'objet d'un chiffrement permettant leur confidentialité[1193]. Les données ne peuvent être stockées plus de 30 jours, délai à l'issu duquel elles sont automatiquement supprimées du serveur[1194]. Aussi, toutes les actions réalisées sont retranscrites dans un journal permettent un traçage des activités comme prévu par arrêté du 24 octobre 2019[1195]. Ces dispositions pour le moins complexes laissent sous-entendre un niveau élevé de sécurisation des données échangées via les plateformes. Sa brièveté permet néanmoins de laisser la place à certaines interrogations sur la pratique et le sort des données traitées[1196]. Présentés comme permettant des échanges importants de données de manière sécurisé, pour notamment remédier aux carences des réseaux privés virtuels.

3° Le traitement dématérialisé des données protégées

401. La communication numérique de données couvertes par un secret – La dématérialisation de la justice passe donc par la numérisation des données de procédure et soulève la question de l'accès à ces données notamment lorsqu'il s'agit de données couvertes par un secret. Si la loi encadre strictement la communication de ces données, la numérisation

[1190] Arrêté du 24 octobre 2019, autorisant la mise en œuvre d'un traitement automatisé de données personnelles dénommé PLINE et PLEX, JORF n°0256, 3 novembre 2019.
[1191] Arrêté du 24 octobre 2019, relatif aux caractéristiques techniques de la communication par voie électronique via la plateforme sécurisée d'échange de fichiers PLINE et PLEX, JORF n°0256, 3 novembre 2019.
[1192] Arrêté du 24 octobre 2019, relatif aux caractéristiques techniques de la communication par voie électronique via la plateforme sécurisée d'échange de fichiers PLINE et PLEX, article 4.
[1193] Arrêté du 24 octobre 2019, relatif aux caractéristiques techniques de la communication par voie électronique via la plateforme sécurisée d'échange de fichiers PLINE et PLEX, article 7.
[1194] Arrêté du 24 octobre 2019, relatif aux caractéristiques techniques de la communication par voie électronique via la plateforme sécurisée d'échange de fichiers PLINE et PLEX, article 8.
[1195] Arrêté du 24 octobre 2019, relatif aux caractéristiques techniques de la communication par voie électronique via la plateforme sécurisée d'échange de fichiers PLINE et PLEX, article 9.
[1196] A. Lecourt, Procédure civile et numérique – La numérisation des actes de procédure ordinaire, Répertoire *IP/IT et communication*, juin 2020. Voir, C. Bléry, J.P. Teboul, Procédure administrative - Télérecours et télérecours citoyen Apports et perspectives en matière de justice numérique, *JCP G*, 23 novembre 2020, 1330. C. Bléry, J.P. Teboul, PLINE et PLEX ou les mystères de la nouvelle « communication par voie électronique », *Dalloz actualité*, 18 novembre 2019. Les auteurs soulèvent notamment des imprécisions quant aux agents autorisés à accéder aux données et sur des imprécisions terminologiques laissant place à des ambigüités et des interrogations.

constitue-t-elle une garantie supplémentaire de sécurité des données ou au contraire un risque majoré de fuite ? A ce sujet, le Syndicat national de la magistrature a alerté sur les risques accrus de fuite de données du fait de la dématérialisation des procédures. Le syndicat vise tout particulièrement le logiciel de chaine pénale « Cassiopée » qui est accessible dans certains cas à des stagiaires ou vacataires présentant selon lui « des garanties de confidentialité très imparfaites »[1197]. Il est vrai que ce public n'est pas soumis au principe de secret issu de l'article 11 du code de procédure pénale et la garantie tient au principe de discrétion contenu dans leur contrat de travail. Partant de ce constat, toute révélation de données couvertes par un secret ne tombe pas sous le coup de l'article 11 du code de procédure pénale. Il n'y a alors pas violation du secret de l'instruction mais seulement faute professionnelle. Néanmoins il faut bien admettre qu'il serait impossible d'œuvrer pour la justice sans avoir accès à aucune donnée. La question peut se poser de savoir si d'autres garanties pourraient être prévues dans ces cas précis ? La garantie existante tient au possible traçage des personnes ayant accès à ces données puisque, par principe, tout accès aux traitements de données judiciaires, se fait par une identification ou authentification individuelle. Ainsi, il est possible, a minima, de savoir quelle personne a accédé au dossier d'enquête ou d'instruction.

Conclusion du titre 1

402. Le secret de l'enquête et de l'instruction : un principe affirmé mais relatif – L'affirmation du principe de secret de l'enquête et de l'instruction tend à assurer une protection générale des pièces de la procédure et par extension des données à caractère personnel contenues dans celle-ci. La protection des données, nécessaire au bon déroulement de l'enquête et la protection des individus et de leur vie privée ou de leur présomption d'innocence, n'en fait pourtant autant pas un principe absolu. Si le principe reste strictement affirmé lors de la phase d'enquête, la phase juridictionnelle d'instruction nécessite la mise en œuvre d'un droit de regard des parties sur la procédure. Aussi, la communication des données d'instruction peut s'avérer nécessaire à l'exercice d'une action civile. Le phénomène de juridictionnalisation de la phase d'enquête tend à étendre ce droit aux individus visés par une enquête et à permettre une diffusion des données avant même la phase d'instruction. Aussi, dans l'optique d'assurer une justice plus transparente à l'égard des justiciables, l'idée d'un

[1197] Syndicat national de la magistrature, « Observations devant la mission parlementaire d'information sur le secret de l'enquête et de l'instruction », *in syndicat-magistrature.org* [en ligne], publié le 26 juillet 2019, consulté le 28 septembre 2020.

droit à l'information ne cesse de croitre imposant de repenser la communication sur les enquêtes et affaires en cours par les autorités judiciaires. Cet exercice s'avère souvent nécessaire du fait de la médiatisation de plus en plus importante des affaires judiciaires. Il n'en reste pas moins un exercice délicat qui impose de chercher l'équilibre entre la diffusion publique de données utiles à l'information à laquelle les justiciables peuvent prétendre et le respect à la fois du bon déroulement de l'instruction et des principes tels que le secret ou la présomption d'innocence. Enfin, une protection n'est effective que si l'incrimination prévue par les textes est appliquée. Il a pu être constaté que la violation du secret de l'enquête et de l'instruction n'était que rarement prononcée amenant une partie de la doctrine à s'interroger sur son réel intérêt ou, du moins, sur sa réelle existence.

403. Le secret professionnel : Une protection relative – Le secret professionnel est souvent présenté comme assurant une protection des données. Il faut rappeler que ce principe soumet le dépositaire à une obligation de silence et est donc attaché à l'individu détenteur. Ce principe a pu s'agissant de certaines professions être présenté comme absolu notamment s'agissant du secret médical. Toutefois, la jurisprudence témoigne de la relativité attachée au secret professionnel. En effet, le secret professionnel ne peut pas être invoqué dans tous les cas pour s'opposer à la divulgation de données qui seraient nécessaires à a résolution d'un litige, soulevant ici la question de sa mise en balance avec le droit à la preuve notamment. Aussi, le secret professionnel ne peut être un obstacle à la justice sauf motif ou empêchement légitimes laissant planer le doute quant à leurs portées respectives.

404. La publicité des données de la procédure et la contradiction : la transparence de la justice aménageable – Par principe la justice est rendue publiquement au nom de sa transparence. Néanmoins le principe peut connaitre des aménagements afin d'assurer la protection de l'ordre public ou d'intérêts privés. Aussi, le recours au témoignage anonyme s'il assure la protection des données identifiantes a pu soulever des interrogations en termes de fiabilité de la preuve et de respect du contradictoire.

405. Interrogations légitimes quant à la généralisation de la dématérialisation – Le mouvement de dématérialisation qui s'est accéléré ces dernières années témoigne de la volonté de moderniser le système judiciaire mais soulève des craintes légitimes. S'agissant des données personnelles, la dématérialisation interroge quant à la sécurité de celles-ci. La question se pose d'autant plus avec le projet, en matière civile d'abord, d'une procédure qui

serait entièrement dématérialisée. On peut aussi s'interroger sur les risques d'un système qui serait entièrement dépendant de l'outil informatique, celui-ci ayant à de maintes reprises démontré ses faiblesses.

Cette question de la dématérialisation des décisions de justice invite à s'interroger sur celle plus générale du sort des données après la procédure et sur le possible droit à l'oubli s'agissant des données collectées dans le cadre d'une procédure judiciaire.

TITRE SECOND

LE SORT DES DONNEES A CARACTERE PERSONNEL COLLECTEES DANS LE CADRE DE PROCEDURES JUDICIAIRES

406. Notion large de traitement – La notion de traitement de données à caractère personnel telle que définie dans le règlement général sur la protection des données renvoie à « toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction »[1198].

S'agissant du traitement de données intervenant dans une procédure judiciaire, les dispositions du règlement général sur la protection des données renvoient en matière de protection des personnes physiques à la directive « Police-Justice » du 27 avril 2016[1199]. Cette dernière a été transposée en droit interne dans la loi informatique et libertés.

L'étude du traitement des données à caractère personnel dans les procédures judiciaires au vu notamment des normes européennes, suppose pour être complète de s'intéresser aux questions attachées à la gestion des données qui ont été collectées et fichées durant la procédure ainsi qu'à leur rectification et effacement. Il s'agit ici de s'interroger sur le traitement de ces données qui ont été collectées au cours d'une procédure

407. Problématiques multiples – La première difficulté du sujet est attachée à la définition même que l'on retient de l'oubli et du droit à l'oubli. Ensuite, retenant une définition large de la notion d'oubli, il apparait que le sujet renvoie à diverses normes avec d'un coté les textes régissant la gestion des données fichées et la protection des individus s'agissant de données traitées pour les besoins de la justice et de l'autre les droits réaffirmés par la loi informatique

[1198] Art. 4 du règlement général sur la protection des données.

[1199] Directive (UE) n°2016/680, du Parlement européen et du Conseil, 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, et abrogeant la décision-cadre 2008/977/JAI du Conseil, *op. cit.*

et libertés s'appliquant aux traitements privés. Enfin, les droits reconnus n'étant pas absolus, il convient de les confronter à d'autres droits et libertés notamment la liberté d'expression ou le droit à l'information, qui constituent des freins à ces derniers.

Le sujet du sort des données personnelles collectées au cours des procédures judiciaires amène d'abord à s'interroger sur la manière dont sont gérées les données une fois le jugement rendu. Cela renvoie aux questions liées à la publicité et à la publication du jugement qui conduisent à diffuser les données qu'il contient. Se pose aussi la question de la gestion des données une fois intégrées dans un fichier judiciaire.

Ensuite, le sujet impose de s'interroger sur la notion d'oubli dans les procédures judiciaires et soulève la question de l'effectivité d'un « droit à » l'oubli. S'agissant des données fichées la question se pose ici de l'effacement au terme du procès. La gestion de ces données répond à des dispositions légales spécifiques relevant notamment du droit processuel et procédural. L'oubli peut renvoyer aussi à la « mémoire collective » et amène à s'interroger sur les droits des individus visés par la procédure sur leurs données.

Il convient donc de s'intéresser à la gestion des données à caractère personnel intervenant dans les procédures judiciaires (Chap.1), pour s'interroger ensuite sur le droit à l'oubli dans le traitement judiciaire des données à caractère personnel (Chap.2).

CHAPITRE 1 : LA GESTION DES DONNEES A CARACTERE PERSONNEL COLLECTEES DANS LE CADRE D'UNE PROCEDURE JUDICIAIRE

408. La gestion des données diffusées – Une fois le jugement rendu (et alors même que la procédure peut se poursuivre via l'exercice des voies de recours), il convient de s'interroger sur la question des données contenues dans la décision. Au-delà du principe de publicité[1200] se pose la question de la diffusion à grande échelle de ces données judiciaires sur des bases de données en libre accès. Ce sujet est plus que jamais d'actualité avec l'ouverture en open data des décisions de justice[1201]. Cette diffusion massive de données et la mise en open data des décisions de justice ont conduit à repenser les normes encadrant cette mise à disposition, tant sur des problématiques de sécurité des données que plus largement sur des préoccupations de respect des droits des individus visés par les traitements. La diffusion et rediffusion des données sur internet soulève évidemment des interrogations quant au possible contrôle effectué sur ces traitements.

409. La gestion des données fichées – La gestion des données collectées dans le cadre d'une procédure judiciaire pose également la question, plus particulière, du sort réservé aux données fichées par les autorités. Des dispositions légales viennent encadrer cette gestion de données en prévoyant notamment des durées de conservation au-delà desquelles les données sont effacées. Certains faits peuvent également justifier un effacement des données, renvoyant ici davantage à l'idée d'une mise à jour des fichiers. La loi encadre de la même manière les flux des données fichées, leur consultation et leurs éventuels transferts. Ainsi, il convient de s'intéresser successivement à la question de la diffusion à grande échelle des décisions de justice (Sect. 1), puis à celle de la gestion des données à caractère personnel fichées (Sect.2).

Section 1 : L'encadrement de la diffusion des décisions de justice

410. La publication pendant du principe de publicité – La publicité renvoie à la garantie procédurale qui pose, sauf exception, le principe d'une audience et d'un jugement publics. Cette notion est entendue très largement notamment s'agissant de la publicité du jugement. En ce sens, la Cour européenne des droits de l'homme admet que la publicité du jugement peut

[1200] V. *supra* n°352 s.
[1201] Loi n°2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice, art. 33. L. Cadiet, Rapport sur l'open data des décisions de justice, novembre 2017.

prendre différentes formes. Les évolutions législatives récentes, tant internes que supra nationales, ont accordé une place plus importante au numérique et ce courant se répercute également sur l'application des principes de droit processuel et notamment celui de la publicité de la justice. Finalement, la notion de publicité s'entend comme le droit pour tout individu de prendre connaissance des décisions rendues posant ainsi un réel droit d'accès à ces dernières. Le numérique a nécessairement bouleversé la mise en œuvre de cette mise à disposition soulevant des interrogations qui jusqu'alors n'avaient pas lieu de se poser. En ce sens, cet accès aux décisions peut être présenté comme le pendant, après la phase du procès, du principe de publicité[1202]. Saisi d'un contrôle a priori de la loi du 23 mars 2019[1203], le Conseil constitutionnel a rappelé la valeur constitutionnelle du principe de publicité[1204]. En effet, initialement le droit d'accès aux décisions est bien distinct du principe de publicité qui découle de la garantie procédurale inhérente au procès. Le terme de publication renvoyait davantage à la diffusion des décisions de justice après le procès. Le développement des nouveaux moyens de communication appelle à s'interroger de manière plus générale sur la mise à disposition des décisions de justice dans ce nouveau contexte qui a poussé à repenser les modalités de diffusion des jugements pour y apporter des garanties suffisantes. La mise à disposition numérique des décisions (§1.) soulève la question de la protection des données à caractère personnel contenues dans les décisions de justice (§2.)

§1. La mise à disposition numérique des décisions de justice

411. L'affirmation d'un droit à l'information – La reconnaissance d'un droit d'accès pour tout justiciable aux décisions rendues trouve sa source dans l'idée générale selon laquelle la justice se doit d'être transparente et ne peut être rendue de manière secrète. Cela renvoie aux dispositions de l'article 15 de la Déclaration des droits de l'Homme et du citoyen de 1789[1205]. On peut également faire un parallèle avec l'émergence du droit d'accès par les individus aux

[1202] C. Bourgeos, Réflexions à propos de l'anonymisation des décisions de justice publiées sur support numérique, *Communication commerce électronique*, juin 2004, n°6, étude 16. Voir, Y. Meneceur, Justice - Open data des décisions de justice Pour une distinction affirmée entre les régimes de publicité et de publication, *JCP E*, 12 septembre 2019, 1415.
[1203] Loi n°2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice.
[1204] Cons. const., 2019-778 DC du 21 mars 2019.
[1205] « La société a le droit de demander compte à tout agent public de son administration ».

documents administratifs[1206] et du droit plus général à l'information[1207]. L'affirmation de ce droit, s'agissant du traitement de données à caractère personnel, recouvre en réalité deux aspects. Face à la consécration d'un droit d'accès numérique aux données judiciaires (A.), il convient de s'interroger sur la mise à disposition des décisions de justice au regard des normes encadrant le traitement de données à caractère personnel (B.).

A. La consécration d'un droit d'accès numérique aux données judiciaires

412. *Open access, open data* – Le droit d'accès aux décisions de justice renvoie en réalité à plusieurs notions qu'il convient avant toute chose de bien distinguer. Dans un premier temps, il renvoie au droit de se voir délivrer par les services de greffe, une copie de toute décision rendue par les juridictions judiciaires ou administratives (*open access*), et dans un second temps à la mise à disposition gratuite des décisions sous format numérique (*open data*). Ces deux notions sont bien distinctes. Cette distinction se retrouve dans la loi du 23 mars 2019 et le décret du 29 juin 2020[1208]. Ainsi, l'article L111-13 du code de l'organisation judiciaire tel que modifié par la loi du 23 mars 2019 vise l'accès aux décisions sous réserve des dispositions relatives à la publicité et l'article L111-14 encadre la diffusion jugements. Partant d'une distinction affirmée entre *open access* et *open data* (1°), on assiste à une multiplication des modes de diffusion des décisions de justice (2°).

1° Une distinction affirmée entre *open access* et *open data*

413. Précisions terminologiques – La notion *d'open data* évoque littéralement les « données ouvertes » c'est-à-dire aux données librement accessibles en format numérique. En cela, il faut bien distinguer les données en *open data* des données dites en *open access* qui renvoient au droit d'accès à une copie du jugement par un tiers et qui permet, de fait, à la mise en œuvre du

[1206] En ce sens, la loi dite « Valter » du 28 décembre 2015 énonce le droit de « demander des comptes » à l'Administration. Néanmoins, cette loi ne vise pas les décisions de justice. Loi n° 2015-1779 du 28 décembre 2015, relative à la gratuité et aux modalités de la réutilisation des informations du secteur public.

[1207] Pour plus de détails sur l'application du droit à l'information, voir, Cour E.D.H. Gde. Chbre., *Axel Springer AG c/ Allemagne*, 7 févier 2012, n°39954/08. Dans cet arrêt le droit à l'information est confronté au droit au respect de la vie privée, l'occasion pour la Cour européenne des droits de l'homme de préciser les critères de mise en balance et d'appréciation des deux. Voir également, Cour E.D.H., Gde. Chbre., *Magyar Helsinki Bizottsàg c/ Hongrie*, 8 novembre 2016, n°18030/11. Voir, G. Puydebois, Le pas mesuré de la Cour européenne des droits de l'Homme vers la reconnaissance d'un droit d'accès à l'information, *Revue JADE*, 1 janvier 2017.

[1208] Décret n°2020-797 du 29 juin 2020 relatif à la mise en open data des décisions judiciaires et administratives.

principe de publicité[1209]. Deux arrêts récents de Cour d'appel soulèvent cette distinction[1210]. L'existence d'un droit d'accès à une copie de jugement gratuite n'est pas récente et a été affirmée dans une loi du 30 décembre 1977 qui instaure la gratuité des actes de justice[1211]. Finalement, la publicité des décisions de justice peut prendre différentes formes et relever à plusieurs régimes. Il peut s'agir de la mise en œuvre classique du principe de publicité par la remise d'une copie de jugement, de la mise à disposition sous format numérique par le biais du service public de diffusion du droit ou de la mise à disposition via internet par des éditeurs privés[1212].

S'agissant du traitement de données à caractère personnel et des interrogations spécifiques soulevées par la diffusion des décisions de justice, il convient de s'intéresser à la mise à disposition numérique de ces décisions. Si le terme *d'open data* semble être aujourd'hui admis pour qualifier la mise à disposition des décisions de justice via internet, certains se sont interrogés sur les fondements réels de la notion. On peut en effet distinguer *l'open data* tel que défini par la loi du 28 décembre 2015, qui exclut par principe les décisions judiciaires, et la notion *d'open data* des décisions de justice issue de la loi du 7 octobre 2016 pour une République numérique. Finalement il convient de distinguer la mise à disposition des jugements sur internet qu'est *l'open data*, et le droit à la remise d'une copie de la décision qui reste toutefois encadré. C'est la première notion qui intéresse particulièrement le sujet et le domaine du traitement des données à caractère personnel, et qui soulève dans sa pratique le plus d'interrogations. En effet, aux cotés des éditeurs classiques se sont développés ce qu'on désigne sous le vocable de « *legal tech* » qui tendent à rendre accessibles beaucoup plus de décisions. Ce phénomène a pris une ampleur considérable notamment depuis l'adoption de la loi pour une République numérique, la loi de programmation du 23 mars 2019 et le décret du 29 juin 2020[1213].

[1209] Sur la distinction voir, N. Fricero, Open Data - Diffusion au public et délivrance aux tiers des décisions des juridictions judiciaires Une mise en œuvre responsable et progressive ! , *JCP G*, 13 juillet 2020, 846. B. Cassar, La distinction en *l'open data* et l'accès aux décisions de justice, *Dalloz actualité*, 19 juillet 2019.

[1210] CA Paris, ch. 1ère, 25 juin 2019, n°19/04407. CA Douai, 21 janvier 2019, n°18/06657.

[1211] Loi n°77-1468 du 30 décembre 1977 instaurant la gratuité des actes de justice devant les juridictions civiles et administratives.

[1212] Pour reprendre la distinction faite par B. Cassar, La distinction entre l'open data et l'accès aux décisions de justice, *op. cit.*.

[1213] Ayant même conduit aux recours engagés par la startup « Doctrine » contre les greffes afin les enjoindre de délivrer les décisions permettant d'alimenter leur base de données sur le fondement des articles 1441, 1440 du code de procédure civile et L-111-13 du code de l'organisation judiciaire. CA Paris, pole2, ch.1, 18 décembre 2018, n°17/22211, CA Douai, 21 janvier 2019, n°18/0665.

414. *L'open data* juridique – *L'open data* a été défini comme les « données qu'un organisme met à la disposition de tous sous forme de fichiers numériques afin de permettre leur réutilisation »[1214] ou encore comme « la politique d'ouverture des données publiques consistant à permettre l'accès à tous dans un objectif de transparence et d'en permettre la réutilisation »[1215]. Cette mise à disposition des décisions de justice a été engagée dès 1985 avec la création du journal officiel électronique[1216] et affirmé ensuite en 1999 avec la création du site Légifrance[1217]. Un décret du 7 aout 2002 pose ensuite le principe d'une mise à disposition gratuite des décisions des Cours suprêmes et du tribunal des conflits[1218].

De cette volonté est né le projet de plateforme Portalis mis en œuvre dans le cadre de la réforme de modernisation de la justice du 21e siècle qui permet au justiciable d'avoir accès à une information juridique fiable et aux documents nécessaires à son action. Le mouvement de mise en *open data* de la justice a été initié par la loi du 7 octobre 2016 dans un but affirmé de transparence de l'Administration et de diffusion des données ayant un intérêt économique, sociale, environnemental ou sanitaire. Cette loi entendait donc faire de la diffusion le principe et du secret l'exception.

S'agissant de la mise en *open data* des décisions de justice, la loi de programmation du 23 mars 2019 et le décret du 29 juin 2020 relatif à la mise à disposition du public des décisions de justice sont venus apporter des précisions. La loi de programmation du 23 mars 2019 est venue compléter les dispositions de l'article L111-13 du code de l'organisation judiciaire qui dispose que « Sous réserve des dispositions particulières qui régissent l'accès aux décisions de justice et leur publicité, les décisions rendues par les juridictions judiciaires sont mises à la disposition du public à titre gratuit sous forme électronique »[1219]. La loi est venue apporter des précisions notamment s'agissant de la protection des données contenues dans les décisions mises à dispositions.

Le décret du 29 juin 2020 prévoit une mise à disposition de toutes les décisions de justice rendues publiquement, sans autorisation préalable[1220].

[1214] Commission générale de terminologie et de néologie, JORF n°0103 du 3 mai 2014, texte n°107.

[1215] Fiche d'orientation, Open data, Dalloz, janvier 2020. La notion renvoie à l'article L.312-1 du code des relations entre le public et l'administration.

[1216] Arrêté du 13 mars 1985 portant dispositions relatives à la création du Journal officiel électronique (JOEL) et sa commercialisation par la direction des journaux officiels, .JORF, 14 mars 1985.

[1217] Arrêté du 6 juillet 1999 relatif à la création du site internet Légifrance, JORF n°160 du 13 juillet 1999.

[1218] Décret n° 2002-1064, du 7 août 2002, relatif au service public de la diffusion du droit par l'internet.

[1219] L'ancien article L111-13 du COJ issu de la loi du 7 octobre 2016 était plus sommaire. Il visait le respect de la vie privée et prévoyait avant la mise à disposition une analyse des risques de réidentification.

[1220] Art. R111-11 du code de l'organisation judiciaire.

Plus précisément, en matière civile sont prononcés publiquement les jugements en matière contentieuse excluant la matière gracieuse, les jugements relatifs à l'état des personnes, les jugements qui touchent à la vie privée des individus ou au secret des affaires[1221]. En matière pénale, les articles R111-10 et suivants du code de l'organisation judiciaire disposent que la Cour de cassation est responsable de la mise à disposition sous forme électronique des décisions. Les dispositions de l'article R111-11 du code de l'organisation judiciaire prévoit toutefois la possible mise à disposition des décisions soumises à autorisation préalable dans le cas où celles-ci présentent un « intérêt particulier ».

Ainsi, l'article L111-13 prévoit l'occultation des noms et prénoms des parties et tiers avant la mise à disposition. Toutefois, lorsqu'il y a un risque pour la sécurité ou la vie privée, le magistrat responsable peut décider de l'occultation de tout élément permettant l'identification des parties, tiers, magistrats ou greffiers à la procédure[1222]. Si initialement n'étaient mises à disposition du public que certaines décisions, le décret vise une diffusion massive des décisions rendues publiquement. Les décisions dont le prononcé n'a pas été public pourront être diffusées selon un critère d'utilité. Une note conjointe de la Chancellerie et de la Cour de cassation est venue préciser le calendrier de mise en œuvre de cette réforme en prévoyant dans un premier temps une mise à disposition des arrêts de cassation pour septembre 2021 puis par la suite une mise à disposition des autres décisions y compris de celles prises antérieurement.

2° La multiplication des modes de diffusion des décisions de justice

415. Nouveaux modes de diffusion, nouvelles problématiques – L'accessibilité aux décisions de justice connait un développement d'une ampleur particulière avec le développement d'internet et la multiplication des *legaltech*, qui conduit à repenser les modalités de diffusion. Aujourd'hui face à la multiplication des acteurs de l'édition juridique, la question de la protection des données à caractère personnel contenues dans les décisions prend une nouvelle ampleur et soulève de nouvelles problématiques. On peut aisément admettre que la diffusion d'un jugement relatant le détail des faits à l'origine du litige puisse porter atteinte à la vie privée des parties. Cette atteinte peut prendre une autre ampleur lorsque

[1221] Voir la loi de programmation du 23mars 2019 qui modifie la loi du 5 juillet 1972 réformant la procédure civile. Voir l'article 451 du code de procédure civile et l'article 1016 du même code qui prévoit le prononcé public des arrêts de Cour de cassation.
Voir, N. Fricero, Open Data, Diffusion au public et délivrance aux tiers des décisions des juridictions judiciaires Une mise en œuvre responsable et progressive !, *op. cit.*
[1222] Art. L111-13 du code de l'organisation judiciaire.

la publication se fait sur internet sur un site rendu accessible au plus grand nombre. Néanmoins, l'atteinte justifie t'elle de retirer toute ou partie des données identifiantes du jugement ? Le phénomène d'ouverture des données judiciaires s'est accompagné d'un développement de nouveaux outils de mise à disposition visant précisément à faciliter la diffusion du droit. Pour autant, le développement des éditeurs privés soulèvent des interrogations qui ne se posaient pas nécessairement lorsque la diffusion émanait soit du service public soit de grands éditeurs privés dont l'accès était limité. Ce développement est la conséquence de l'affirmation d'un droit à l'information du public s'agissant des données judiciaires[1223].

Le développement des bases de données jurisprudentielles étatiques numériques dans un premier temps avec des accès limités, puis le développement des *legalthech*, poussent à s'interroger sur la question de la protection des données diffusées. Face au développement de la concurrence, les éditions Dalloz ont par exemple décidé en octobre 2016 de mettre une partie de leur fond de jurisprudence en libre accès[1224]. Avec les lois récentes visant la mise à disposition massive d'une partie des décisions de justice et l'affirmation d'une mise en *open data* pour tous, de nombreux autres éditeurs tendent à se développer soulevant d'autant plus des interrogations en termes de protection des données mais avant tout en termes de traitement de données à caractère personnel.

B. La mise à disposition des décisions de justice au regard des normes encadrant le traitement de données à caractère personnel

416. La mise à disposition des décisions de justice, un traitement de données à caractère personnel – Face au développement de nouveaux moyens de diffusion on peut s'interroger sur l'application des normes encadrant le traitement de données à caractère personnel en la matière. Les sites internet permettant la diffusion des décisions de justice constituent des traitements de données au sens de la loi informatique et liberté et du règlement général sur la protection des données en ce qu'ils permettent la collecte, l'enregistrement et la diffusion de données identifiantes. En effet les jugements mis à disposition du public contiennent sauf

[1223] De manière plus générale, le droit à l'information a été reconnu par la Cour européenne des droits de l'homme. Cette dernière a consacré le principe en vertu duquel la révélation de données privées peut être légitime si le sujet relève d'un intérêt général. La Cour européenne des droits de l'homme vise l'intérêt légitime du public. Cour E.D.H., gr. ch. 10 novembre 2015, *Couderc et Hachette Filipacchi associés c/ France*, n°40454/07.

[1224] C. Sztejnhorn, L'open access et l'édition juridique : l'exemple de la disruption open Dalloz, *Dalloz IP/IT*, 2017,p.97.

exception des données qui peuvent permettre indirectement l'identification des individus concernés. L'occultation des noms et prénoms ne suffit pas nécessairement à rendre les parties non identifiables au vu d'autres éléments contenus dans le jugement tels que lieux géographique, l'emploi... L'enjeu est donc de concilier protection des données à caractère personnel et mise à disposition des décisions. Les récentes lois ayant réaffirmé certains principes s'agissant des traitements de données à caractère personnel, il convient tout d'abord de s'interroger sur les questions entourant la mise à disposition des décisions au regard du principe de licéité du traitement (1°) puis au regard des droits des individus visés par le traitement (2°).

1° La mise à disposition des décisions au regard du principe de licéité du traitement

417. Les bases légales justifiant un traitement de données à caractère personnel – L'article premier de la loi informatique et libertés dispose que « l'informatique doit être au service de chaque citoyen » et ne doit pas porter atteinte à la vie privée ou aux libertés individuelles. Si l'on observe les conditions de licéité du traitement posées par l'article 5 de la même loi, il ressort que pour être licite tout traitement doit soit reposer sur le consentement de la personne visée soit répondre à une des conditions posées. Ces conditions renvoient notamment aux traitements relevant d'une autorité publique ou répondant à des intérêts légitimes.

418. La licéité du traitement au regard de la nature des données à caractère personnel traitées – L'article 6 de la loi informatique et liberté pose le principe de l'interdiction de traitement des données relatives aux opinions, aux convictions ou aux données génétiques par exemple. Limites qui connaissent néanmoins des exceptions s'agissant notamment des traitements 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[1225]. L'article 44 de la loi informatique et libertés précise que les dispositions de l'article 6 ne s'appliquent pas s'agissant des « réutilisateurs » visés à l'article L111-13 du code de l'organisation judicaire[1226].

La loi pose également des conditions particulières s'agissant du traitement de données relatives à des condamnations pénales en précisant à l'article 46 de la loi informatique et

[1225] Art. 44 de la loi informatique et libertés.
[1226] Art. 44 5° de la loi informatique et libertés.

libertés que celui-ci ne peut être mis en œuvre que par une autorité publique ou une juridiction. Aussi, le même article prévoit la possibilité de traitement des données relatives aux condamnations par les « réutilisateurs » à la condition toutefois de ne pas pouvoir réidentifier les individus visés. La loi informatique et libertés renvoie ainsi aux dispositions de l'article L111-13 du code de l'organisation judiciaire[1227]. Au vu de ces dispositions on peut s'interroger sur la légalité des bases de données relatives aux décisions de justice, ces dernières comportant nécessairement outre les données relatives à la décision, des données à caractère personnel parfois sensibles ou dont le traitement est par principe prohibé. Ces interrogations se posent d'autant plus que la diffusion peut être mise en œuvre par des éditeurs privés ne relevant pas de l'autorité publique ayant pris la décision. La Commission nationale de l'informatique et des libertés s'était prononcée sur cette question dans son bilan d'application de la recommandation en date du 29 novembre 2001[1228]. Elle a alors rappelé les dispositions des articles 5 et 6 de la loi informatique et libertés posant les conditions de licéité du traitement de données. Si la Commission a alors admis que le traitement mis en œuvre par les autorités publiques relève des dispositions de la loi, en revanche, ces dispositions ne visent pas les bases de données jurisprudentielles mises en œuvre par un éditeur privé. En conséquence, la CNIL considère que ces derniers doivent obligatoirement occulter les données à caractère personnel des décisions qu'ils publient[1229]. En ce sens le règlement européen relatif à la protection des données suggère la mise en œuvre de moyens visant à assurer une protection renforcée des données à caractère personnel, comme la pseudonymisation lorsque ces dernières sont conservées à des fins archivistiques notamment ou statistiques. Le sujet soulève donc évidemment la question de la protection de ces données relatives aux décisions de justice conservées et mises à disposition du public et des conditions de cette mise à disposition au vu notamment des normes encadrant le traitement de données à caractère personnel. Se pose en toile de fond la problématique de la recherche d'équilibre entre la protection des données à caractère personnel contenues dans les décisions et le droit à l'information affirmé par leur mise en *open data*.

[1227] Art 46 5° de la loi informatique et libertés.

[1228] Bilan de l'application de la recommandation de la CNIL du 29 novembre 2001 sur la diffusion de données personnelles sur Internet par les banques de données de jurisprudence : pour un encadrement législatif renforçant la protection des données à caractère personnel en matière de diffusion de décisions de justice. Adopté par la commission le 19 janvier 2006. 7 pages.

[1229] *Ibid*. Dans sa recommandation en date du 29 novembre 2001, la CNIL n'avait pas jugé utile de préconiser une quelconque anonymisation des décisions avant leur publication en format numérique puisque à l'époque ces bases de données avaient un public restreint et l'accès était payant.

2° La mise à disposition des décisions au regard des droits des individus visés par le traitement

419. L'application des principes protecteurs des données à caractère personnel – La protection des données à caractère personnel passe également par la reconnaissance de droits attribués aux individus visés par un traitement. Ces droits ont été réaffirmés récemment dans le règlement européen sur la protection des données et par la loi informatique et libertés. La mise à disposition des décisions de justice via différents sites internet permettant leur conservation et leur diffusion constitue un traitement de données au sens du droit européen et du droit interne. Il s'agit donc de s'interroger sur l'application faite de ces principes protecteurs s'agissant des bases de données jurisprudentielles. Dans deux délibérations en date du 19 juillet 2012, la CNIL rappelle que le droit d'opposition ne trouve pas à s'appliquer s'agissant des bases de données jurisprudentielles gérées par les autorités publiques et qui répondent à une obligation légale. Néanmoins, existe un droit à demander l'occultation de certaines données[1230]. La question se pose d'autant plus s'agissant de données personnelles judiciaires traitées par les organismes privés notamment. En effet les normes européennes et internes fixent des droits s'agissant du traitement des données à caractère personnel aux individus concernés.

420. Les droits des personnes visés par le traitement – Le règlement général sur la protection des données et la loi informatique et libertés aux articles 48 et suivants posent, pour les individus visés, un droit d'information, d'accès, de rectification et d'opposition s'agissant du traitement de données à caractère personnel les concernant. La question de l'application du droit d'opposition trouve particulièrement à se poser s'agissant de la mise en *open data* des décisions de justice. Les dispositions de l'article 21 du règlement prévoient néanmoins l'existence de motifs « légitimes et impérieux » permettant de continuer à traiter les données malgré l'exercice du droit d'opposition et vise notamment la constatation, l'exercice ou la défense de droits en justice[1231]. La question est donc de savoir si, au vu de ces dispositions, une personne peut s'opposer au traitement de données la concernant et plus précisément à la publication d'une décision de justice sur une base de données numérique librement accessible.

[1230] En effet, l'intérêt public ou la mission d'intérêt public justifient le traitement de données à caractère personnel et ce même s'agissant de données dont le traitement est interdit. Voir les articles 5 et 6 de loi informatique et libertés. La CNIL est allée dans ce sens dans ses délibérations du 19 juillet 2012 (2012-245 et 2012-246). Selon elle, le droit d'opposition ne trouve pas à s'appliquer s'agissant des bases de données jurisprudentielles gérées par les autorités publiques et qui répondent à une obligation légale.

[1231] Les dispositions de l'article 21 visent les cas de licéité du traitement prévues à l'article 6 §1 e) et f).

La jurisprudence semble défendre le droit à l'information du public. Dans un arrêt du 12 mai 2016, la Cour de cassation a estimé que le fait de supprimer les données identifiantes dans un moteur de recherche sur le site d'un organe de presse était de nature à nuire à la liberté de celle-ci et excédait donc les limitations possibles au droit de la presse[1232].

Dans le rapport remis au garde des sceaux en novembre 2017 par la mission d'étude relative à *l'open data* des décisions de justice[1233], a été abordée la question de la réutilisation des décisions. Si le règlement européen sur la protection des données semble ne pas s'opposer à la réutilisation des données[1234] le risque demeure celui lié à la ré-identification des individus visés dans les décisions. Il faut en la matière citer la décision de la Commission national de l'informatique et des libertés en date du 30 aout 2011, confirmée par le Conseil d'Etat, par laquelle elle a prononcé une sanction à l'encontre d'une base de données jurisprudentielles pour non respect du droit d'opposition. L'association qui mettait en ligne les décisions avait été enjointe d'anonymiser ces dernières[1235]. La loi du 7 octobre 2016 prévoyait déjà qu'une attention particulière soit portée sur les risques de ré-identification. En ce sens, l'article 44 de la loi informatique et liberté prévoit la non-application des dispositions de l'article 6 de la loi relatives aux critères de licéité du traitement lorsque celui-ci porte sur la rediffusion des décisions de justice telle que visée à l'article L111-13 du code de l'organisation judiciaire. Ces dispositions ne sont toutefois applicables qu'à la condition que la rediffusion ne vise ou ne permette pas la ré-identification des individus concernés. L'article 46 de la loi informatique et libertés reprend les mêmes conditions en affirmant que si les « réutilisateurs » visés à l'article L111-13 du code de l'organisation judiciaire peuvent traiter des données pénales liées aux condamnations ou aux infractions, ce traitement ne peut avoir pour but ou conséquence la ré-identification des individus.

La loi du 23 mars 2019 et le décret du 29 juin 2020 prévoient que la mise à disposition du public des décisions de justice doit être précédée d'une analyse des risques de ré-identification. De prime abord donc, rien ne semble exclure le droit pour la personne visée par le traitement de faire jouer son droit d'opposition au traitement. Le décret du 29 juin 2020 relatif à la mise à disposition du public des décisions des juridictions judiciaires et administratives ne fait néanmoins pas référence à ce droit. L'article 8 du décret vise les droits

[1232] Cass., civ. 1ère, 12 mai 2016, pourvoi n°15-1.729. Sans aborder la question du droit au déréférencement et du droit à l'oubli, cet arrêt est intéressant en ce qu'il met en balance le droit à l'information et le droit de s'opposer au traitement de ses données à caractère personnel. Voir, C. Féral-Schuhl, *Cyberdroit, le droit à l'épreuve de l'internet*, *op. cit*., p. 252 et s.

[1233] L. Cadiet, Rapport sur l'open data des décisions de justice, novembre 2017, *op. cit.*

[1234] Art. 6 du règlement général sur la protection des données.

[1235] CE, 10e et 9e ss., 23 mars 2015, n°353717.

d'accès et de rectification qui peuvent être mis en œuvre auprès de la Cour de cassation ou du Conseil d'Etat, responsables du portail permettant la mise à disposition des décisions de justice[1236]. Le décret instaure néanmoins le droit pour les individus visés par le traitement de demander l'occultation de données supplémentaires à celles déjà prévues par les textes[1237]. En tout état de cause, seule une anonymisation stricte peut justifier que soient écartés les droits posés par le règlement général sur la protection des données, puisque si la décision ne comporte plus de données identifiantes elle ne relève donc plus du champ d'application du règlement. De cette question, qui sera abordée plus loin, dépend donc l'application faite ou non de ces dispositions. Le décret du 29 juin 2020 place la mise à disposition des décisions sous la responsabilité des Cours suprêmes s'agissant de la mise en *open data* sur le portail dépendant des juridictions et le décret précise les droits dont disposent les personnes eu égard à ce traitement. Néanmoins reste ouverte la question de l'exercice de ces droits s'agissant des données récupérées puis traitées par des éditeurs privés. La réponse dépend notamment du degré d'occultation des données contenues dans les décisions de justice.

§2. La protection des données à caractère personnel contenues dans les décisions de justice diffusées

421. Nécessaire équilibre entre protection des données et lisibilité des décisions – Indépendamment du mode de diffusion des jugements, la problématique sous jacente reste celle de la protection des données à caractère personnel contenues dans les décisions. Une fois encore, différents intérêts se trouvent en concurrence avec d'un côté les données personnelles des parties au procès et de l'autre l'intérêt affirmé d'accéder à des décisions lisibles. Il faut alors s'interroger sur la nécessité de publier les décisions dans leur intégralité et sur la nécessité d'assurer la protection des individus visés par les jugements. Sous couvert de protection de la vie privée ou de protection des données à caractère personnel, le législateur a développé des procédés visant à assurer cette protection. Souvent regroupé sous le vocable « d'anonymisation », il convient toutefois de faire la distinction entre la protection des données à caractère personnel par l'anonymisation des décisions de justice qui est affirmée depuis longtemps en droit interne (A.) et la protection assurée par la pseudonymisation qui est

[1236] Art. 7 du décret n°2020-797 du 29 juin 2020 relatif à la mise en open data des décisions judiciaires et administratives.
[1237] Art. R111-13 du code de l'organisation judiciaire.

prônée par les instances européennes, pour enfin s'intéresser plus en détails sur le système de protection initié par la loi du 23 mars 2019 (C.).

A. La protection des données à caractère personnel par l'anonymisation des décisions de justice

422. Le débat récent de l'anonymisation des décisions – L'anonymisation par référence au terme d'anonymat, renvoie au procédé qui permet qu'un fait ou un acte ne soit plus associé à son identité. L'anonymisation des décisions de justice n'a pas toujours soulevé de débat comme c'est le cas depuis quelques années. Evidemment, à l'époque où internet commençait son ascension, on ne parlait pas encore de *big data* et les données juridiques n'étaient pas accessibles au plus grand nombre. Il ne fait nul doute que le développement d'internet et plus encore l'émergence de nouvelles bases de données juridiques ont soulevé des interrogations qui semblaient jusque là dérisoires. D'ailleurs, tout étudiant a en tête grand nombre d'arrêts qu'il cite en faisant référence aux noms des parties à l'instance. Par la suite, les procédés d'anonymisation se sont développés mais ils n'étaient souvent que parcellaires et quelques recherches pouvaient permettre d'identifier aisément les parties.

423. Les prémices d'une réflexion relative à la protection de la vie privée dans le traitement de données – Si la loi informatique et libertés du 6 janvier 1978 s'applique aux bases de données juridiques, elle ne fait que très peu référence au processus d'anonymisation des données. C'est véritablement la directive européenne de 24 octobre 1995 qui va poser les bases de la réflexion engagée sur la question de l'anonymisation. Le rapport « Braibant », remis le 3 mars 1998, relatif à la transposition de la directive de 1995 soulevait la question des risques liés au traitement massif de données à caractère personnel. Sans omettre les avancées rendues possibles par internet et le traitement automatisé des données, le rapport s'interrogeait sur les risques d'atteinte à la vie privée et au-delà, aux données à caractère personnel, cette notion étant plus large que celle de vie privée[1238]. Par la suite de nombreux travaux ont été réalisés sur la question, soulevant toujours, et encore aujourd'hui, des divergences d'opinion[1239]. Cette question de la protection de la vie privée dans la publication des décisions

[1238] Rapport Braibant, Données personnelles et société de l'information, 3 mars 1998, p.7.
[1239] E. Lesueur De Givry, *La question de l'anonymisation des décisions de justice*, *in*, Rapport annuel de la Cour de cassation, 2000, Doc. Fr., 2000.

de justice s'est notamment posée s'agissant de la médiatisation de certaines affaires et de la reprise par certains médias de données permettant l'identification des personnes concernées.
Si l'article 39 alinéa second de la loi du 29 juillet 1881 impose d'anonymiser les décisions publiées dans les médias lorsque celles-ci touchent des litiges relatifs à des faits de diffamation, à la filiation, aux actions aux fins de subsides, aux divorces, aux annulations de mariage ou à l'avortement, la CNIL a très tôt abordée la question. Dans une délibération de 1995, cette dernière précisait que la diffusion numérique et gratuite des décisions de justice n'était pas « indispensable » aussi, elle rappelait à cette occasion que « les aménagements aux règles de la protection des données que commande le respect de la liberté d'expression ne doivent pas avoir pour effet de dispenser les organismes de la presse écrite ou audiovisuelle, lorsqu'ils recourent à des traitements automatisés, de l'observation de certaines règles »[1240].
Dans une délibération du 29 novembre 2001, la Commission nationale de l'informatique et des libertés suggérait que soit engagée une réflexion relative à la déontologie des organes de presse s'agissant de la publication de données du procès qu'il s'agisse de publication des décisions de justice ou de compte-rendu d'audiences[1241].
Force est de constater que la mise en *open data* des décisions conduit à repenser l'équilibre entre les différents intérêts en présence, ce dernier étant dès lors plus difficile à trouver. Bien que des moyens existent au préalable sur le terrain notamment de la vie privée, ce nouveau contexte soulève la question de la nécessité de revoir et d'adapter les normes protectrices en la matière[1242].

424. Les modalités d'anonymisation suggérées par la commission nationale de l'informatique et libertés – Dans sa délibération du 29 novembre 2001, la CNIL suggérait aux éditeurs de bases de données jurisprudentielles de ne pas faire apparaitre les noms et adresses des parties et témoins. En revanche, la commission considérait qu'il n'était pas nécessaire d'occulter les noms des magistrats et professionnels intervenant dans la décision sur le fondement de la protection de leur vie privée. Dans son bilan annuel établi en 2006, la CNIL a considéré que ses recommandations avaient été suivies notamment par le principal

[1240] Délibération CNIL, n°95-012 du 24 janvier 1995 portant recommandation relative aux données personnelles traitées ou utilisées par des organismes de la presse écrite ou audiovisuelle à des fins journalistiques et rédactionnelles. Voir, C. Féral-Schuhl, *Cyberdroit, le droit à l'épreuve de l'internet*, *op. cit*., p. 255 et s.
[1241] Voir, A. Lepage, Anonymisation des décisions de justice, *Communication commerce électronique*, n°2, février 2002, comm. 29.
[1242] C. Féral-Schuhl, *Cyberdroit, le droit à l'épreuve de l'internet*, *op. cit*, p. 255 et s.
L'auteure rappelle que si les dispositions de l'article 226-1 du code pénal incrimine l'atteinte volontaire à l'intimité de la personne cette réponse au vu du contexte moderne n'est plus « appropriée ».

site de diffusion du droit « Légifrance ». Néanmoins, elle a appelé à renforcer les moyens de protection des données notamment par la mise en œuvre de systèmes encadrant l'accès aux bases de données. Le libre accès nécessitait selon elle une anonymisation totale des décisions. La commission relevait toutefois à l'époque qu'une anonymisation totale pouvait nuire à la compréhension de la décision et donc constituer un frein aux recherches jurisprudentielles. Finalement, ressort de cette recommandation et du bilan de la CNIL l'idée selon laquelle la mise à disposition des décisions de justice suppose une anonymisation de ces dernières qui nécessite l'occultation des noms et adresses des individus. Ce raisonnement a pu à l'époque sembler rapide comme faisant une application tronquée du processus d'anonymisation et soulève dès lors la question de la définition même de la notion[1243].

425. De la notion d'anonymisation – La recommandation de la CNIL en matière d'anonymisation amène à s'interroger sur la notion même. L'anonymisation peut être définie comme le « processus consistant à traiter des données à caractère personnel afin d'empêcher totalement et de manière irréversible l'identification d'une personne physique. L'anonymisation suppose donc qu'il n'y ait plus aucun lien possible entre l'information concernée et la personne à laquelle elle se rattache. L'identification devient alors totalement impossible»[1244]. La notion d'anonymisation renvoie donc à un processus permettant de ne pas identifier ou réidentifier les individus, ce processus devant être irréversible. C'est cette notion d'irréversibilité qui distingue l'anonymisation de la pseudonymisation[1245].

Si dans les années 80 la CNIL estimait que la suppression de l'identité des individus dans les jugements présentait peu d'intérêts au vu du nombre restreint de personnes qui consultaient ces derniers, la diffusion massive sur des bases de données gratuites a conduit à repenser son utilité[1246].

Cette anonymisation peut prendre différentes formes. Dans son considérant 26, la directive du 24 octobre 1995 visait l'anonymisation des décisions comme moyen ne permettant plus d'identifier les personnes au regard de « l'ensemble des moyens susceptibles d'être raisonnablement mis en œuvre ». Si cette directive a depuis été abrogée, il est toutefois intéressant d'observer les dispositions posées à l'époque ainsi que l'interprétation qui a pu en être faite. Dans son avis du 10 avril 2014, le groupe de travail G29 a dégagé trois critères

[1243] A. Debet, Données personnelles, droit à l'oubli et droit à l'information du public, *in*, La jurisprudence dans le mouvement de l'open data, *JCP G*, supplément n°9, 27 février 2017, p. 37.
[1244] Avis 05/2014 du G29 sur les techniques d'anonymisation.
[1245] V. *infra* n°427.
[1246] Voir sur la question, A. Lepage, Anonymisation des décisions de justice, *Communication commerce électronique*, *op. cit.*

cumulatifs d'anonymisation. Le critère d'individualisation qui permet de voir si l'individu peut toujours ou non être individualisé. Le critère de corrélation qui permet d'observer s'il est toujours possible de relier plusieurs données relatives à l'individu entre elles. Enfin, le critère d'inférence qui s'interroge sur la possibilité de déduire des informations à partir de celles connues. Ainsi, en fonction de ces recommandations, l'anonymisation renvoie aux données qui ne permettent ni d'individualiser, ni de corréler ou d'inférer. Le groupe de travail fait référence aux deux techniques d'anonymisation que sont la randomisation et la généralisation. La randomisation vise de manière générale à « altérer la véracité des données » par différents procédés alors que la généralisation vise à « diluer » la donnée en modifiant son échelle. Quel que soit le mode d'anonymisation retenu, le groupe de travail alerte sur les failles que présente chacun d'entre eux et préconise à l'époque une application au cas par cas.

426. Les conséquences de l'anonymisation – La question de l'opportunité d'anonymiser les décisions de justice avant leur publication soulève aujourd'hui encore de divergences d'opinion. Il a pu être mentionné dans la doctrine que peu de pays de l'Union européenne ont recours à l'anonymisation des décisions de justice. Aussi, a pu être avancé l'argument selon lequel le fait de ne pas occulter l'identité des individus dans les jugements pourrait aboutir à la création d'une forme de « casier juridique »[1247] sur lequel les autorités n'auraient aucun contrôle[1248]. Un autre argument en faveur de l'anonymisation des décisions de justice a été mis en avant par certains magistrats s'agissant de la question plus précise de l'occultation de leur nom dans les jugements. Ces derniers invoquent le fait qu'en révélant leur identité cela pourrait conduire à la réalisation de statistiques relatives à leur manière de statuer[1249]. L'argument invoqué en faveur de l'anonymisation repose le plus souvent sur des préoccupations de protection de la vie privée des parties[1250]. Cet argument a pu être écarté du fait des facilités offertes aujourd'hui qui permettent d'identifier les individus par une recherche effectuée à partir des autres éléments de la décision[1251]. Se pose plus particulièrement la question de l'utilité de faire apparaitre dans la jurisprudence des données

[1247] C. Bourgeos, Réflexions à propos de l'anonymisation des décisions de justice publiées sur support numérique, *Communication commerce électronique, op. cit.* Plus précisément, l'auteur fait référence au fait que sans occultation du nom, une recherche par le nom pourrait conduire à faire ressortir toutes les décisions dans lesquelles l'individu intervient, constituant ainsi une forme de casier.
[1248] *Ibid*.
[1249] M. Léna, Open data : un équilibre délicat, *AJ pénal*, 2020, p.4. C. Fleuriot, Avec l'accès gratuit à toute la jurisprudence, des magistrats réclament l'anonymat, *Dalloz actualité*, 6 février 2017.
[1250] *Ibid*.
[1251] N. Blanc, P.Y. Gautier, Contre « l'anonymisation » des arrêts publiés : décadence des références de jurisprudence, *Recueil Dalloz* 2019, p.1648. Les auteurs soulèvent aussi le fait que d'autres moyens de protection existent déjà notamment dans certains domaines comme en droit des mineurs ou en droit pénal.

identifiantes. Une partie de la doctrine fait référence au risque de « deshumanisation de la justice »[1252]. L'anonymisation des décisions pourrait selon elle nuire à « l'identité des décisions »[1253] les rendant de fait moins remarquables et moins lisibles, soulevant ainsi la question de la finalité de la jurisprudence dans ce nouveau système[1254]. Il faut également noter que l'anonymisation visant à occulter totalement l'identification des individus et à rendre impossible leur identification, on peut considérer que cela revient à occulter toute donnée à caractère personnel. En conséquence, une décision ne comportant plus de données à caractère personnel-ne relève plus des dispositions européennes prises en la matière contrairement aux décisions pseudonymisées.

B. La protection des données à caractère personnel contenues dans les décisions de justice par la pseudonymisation

427. La notion de pseudonymisation – Le premier écueil à éviter serait de confondre anonymisation et pseudonymisation. En effet, les deux notions sont bien distinctes et plus encore renvoient à des régimes différents. Le groupe de travail G29 a déjà alerté sur ce risque de confusion dans son avis de 2014, précisant que « la pseudonymisation n'est pas une méthode d'anonymisation. Elle réduit simplement la corrélation d'un ensemble de données avec l'identité originale d'une personne concernée et constitue par conséquent une mesure de sécurité utile ». En ce sens, le groupe de travail définit la pseudonymisation comme le mécanisme qui « consiste à remplacer un attribut (généralement un attribut unique) par un autre dans une base de données. La personne physique est donc toujours susceptible d'être identifiée indirectement; par conséquent, la pseudonymisation ne permet pas, à elle seule, de produire un ensemble de données anonymes. Elle est néanmoins examinée dans le présent avis en raison de nombreuses idées fausses et erreurs qui entourent son utilisation. La pseudonymisation est consacrée en droit européen. Le règlement général sur la protection des données pose pour la première fois une définition légale et fait référence au « 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 »[1255]. Cette notion est donc bien distincte de celle d'anonymisation puisque l'identification des individus

[1252] *Ibid*.
[1253] *Ibid*.
[1254] Sur la question, voir, P. Deumier, Une autre jurisprudence ?, *JCP G*, n°10, 9 mars 2020, doctr. 277.
[1255] Règlement (UE) 2016/679 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, art. 4 5).

reste possible par recoupement de données. Le groupe de travail G29 fait référence là aussi à différents moyens de pseudonymisation tels que le hachage, la cryptographie, le chiffrement ou la tokenisation[1256]. Le règlement général sur la protection des données vise quant à lui des méthodes telles que le scorage, le masquage ou le caviardage[1257]. Le rapport sur l'open data des décisions de justice remis en 2017 s'est également attaché à distinguer les deux notions[1258]. A partir des définitions posées, le rapport semble affirmer que les décisions mises à disposition sur Légifrance par exemple relèvent d'une pseudonymisation et non d'une anonymisation qui reste difficile à obtenir au vu des technologies modernes. Le rapport suggérait de fixer des règles de pseudonymisation en fonction notamment de la nature des données traitées. Les auteurs considéraient que cette anonymisation ne pouvait pas reposer sur la seule occultation des noms et adresses.

C. Le régime de protection des données initié par la loi du 23 mars 2019

428. L'harmonisation des régimes –Initialement, la délivrance d'une copie de jugement (*open access*) ne supposait pas d'occulter certaines données contrairement à la mise à disposition numérique. La loi du 23 mars 2019 est venue établir une certaine harmonisation de ces régimes en prévoyant dans tous les cas une occultation des données permettant l'identification des individus visés dans les décisions à la charge des greffes. Plus précisément, s'agissant de l'accès aux décisions, les données identifiantes relatives aux individus dont il est fait mention dans le jugement sont occultées, par les greffes, en cas d'atteinte potentielle à leur sécurité ou à leur vie privée[1259]. Les jugements mis à disposition sont diffusés après occultation des noms et prénoms, *a minima,* et éventuellement de données supplémentaires. La loi du 23 mars 2019 a dans un premier temps apporté des précisions quant à la protection des donnés s'agissant du droit d'accès aux décisions (1°), puis elle a précisé les mesures de protection des données contenues dans les jugements diffusés en *open data* (2°).

[1256] La tokenisation par exemple vise à remplacer une données sensibles par une autre qui de fait n'est en l'état pas exploitable.
[1257] La méthode de caviardage vise simplement à occulter les éléments sensibles.
[1258] L. Cadiet, Rapport sur l'open data des décisions de justice, novembre 2017, *op. cit.*, p. 35 et s.
[1259] Art. L111-14 du code de l'organisation judiciaire.

1° La protection des données à caractère personnel dans l'accès aux décisions

429. Précisions quant au droit d'accès – L'accès aux tiers aux jugements relève bien d'un droit et, par principe, le greffe doit y accéder dans un délai de deux mois[1260]. Pour autant, ce droit est limité. La loi de programmation 2018-2022 et de réforme pour la justice du 23 mars 2019 est venue apporter des précisions quant à des litiges nés de situations dans lesquelles des éditeurs se sont vu refuser des copies de jugements. Face aux demandes croissantes d'accès aux jugements, la loi du 23 mars 2019 met un terme aux interrogations quant à l'étendue du droit. Ainsi, en matière d'accès aux décisions, la loi met un certain frein aux demandes en prévoyant que ce droit d'accès aux tiers à une copie ne peut résulter de demandes « abusives »[1261]. Ce caractère abusif renvoie notamment à des demandes qui seraient trop nombreuses, répétitives ou systématiques[1262]. Ces dispositions visent à éviter des demandes qui seraient systématiques et difficiles à satisfaire. Certains invoquent aussi l'idée selon laquelle cette limitation vise à éviter la constitution par des éditeurs privés de base de données contenant toutes les décisions et qui reviendrait pour ces tiers à constituer « leur propre open data »[1263].

430. La remise de copie au tiers – En matière civile, l'article 1440-1-1 du code de procédure civile prévoit désormais une occultation, par le greffe, des éléments permettant l'identification des parties ou des tiers avant toute mise à disposition, lorsque la révélation de ces données peut porter atteinte à leur sécurité ou au respect de leur vie privée ou celle de leurs proches. En matière pénale, l'article R166 du code de procédure pénale prévoit la remise aux tiers, sans autorisation préalable, de copies des arrêts de cassation et des décisions de première instance ou de second degré à la condition qu'elles soient définitives et aient été rendue publiquement. Néanmoins, le procureur de la République ou le procureur général peuvent décider de l'occultation de certaines données permettant l'identification des individus mentionnés dans la décision en cas de risque pour leur sécurité ou leur vie privée[1264]. Aussi les arrêts de Cour d'assises remis à des tiers ne doivent pas comporter le nom des jurés, et les décisions des tribunaux pour enfants ne mentionnent pas le nom des assesseurs[1265]. En matière de crimes et

[1260] Art. 1440 du code de procédure civile.
[1261] Art. L111-14 du code de l'organisation judiciaire.
[1262] Loi n°2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice, art. 33.
[1263] N. Fricero, Open Data - Diffusion au public et délivrance aux tiers des décisions des juridictions judiciaires Une mise en œuvre responsable et progressive ! , *op. cit.*
[1264] Art. R168 du code de procédure pénale.
[1265] Art. R169 du code de procédure pénale.

délits contre les intérêts de la nation ou de criminalité et délinquance organisées, le nom des personnes ayant concouru à la procédure, à l'exception des magistrats et des greffiers, n'apparait pas[1266]. La loi laisse aux juridictions une marge d'appréciation s'agissant de l'opportunité d'occulter certains éléments autres que le nom. Cela peut aussi résulter de demandes formulées par les parties elles-mêmes. Toutefois, ce texte ne prévoit pas de manière systématique l'occultation du nom des magistrats et des greffiers

2° La protection des données à caractère personnel contenues dans les jugements diffusés en open data

431. L'occultation des données identifiantes relatives aux parties – L'article L111-13 du code de l'organisation judiciaire prévoit l'occultation des noms et prénoms des personnes physiques mentionnées dans le jugement avant leur mise à disposition. Les décisions rendues publiquement pourront être par principe mise à disposition en suivant les règles d'occultation fixées. Le décret du 29 juin 2020 est venu harmoniser le régime de mise à disposition des décisions de justice qu'il s'agisse de la remise de copie aux tiers ou de la mise à disposition massive et gratuite en format numérique. Il prévoit plusieurs niveaux de protection. Finalement, le décret portant application des dispositions de l'article 33 de la loi du 23 mars 2019 ne fait pas explicitement référence à l'anonymisation ou à la pseudonymisation des données contenues dans les décisions de justice. Il est question d'occultation des données permettant l'identification des individus visés dans les décisions dans le but de concilier publicité et vie privée des individus. En tout état de cause, le texte fait référence aux données identifiantes soit aux données à caractère personnel telles que visées dans le règlement général sur la protection des données et la loi informatique et libertés et ne semble pas viser une anonymisation au sens strict du terme. On peut en ce sens citer le « projet Open justice » mené conjointement par la Cour de cassation et Etalab[1267] qui vise à développer des moyens fiables permettant de pseudonymiser les décisions et ainsi leur mise en *open data* tout en permettant la réutilisation de ces données par le recours à l'intelligence artificielle. A ce sujet, la Commission de l'Union européenne a publié le 19 février 2020 un livre blanc relatif à

[1266] *Ibid*.
[1267] Administration publique au sein de la Direction interministérielle du numérique dont les missions sont fixées par le décret n° 2019/1088 du 25 octobre 2019. Il coordonne le « service publique de la donnée ».

l'intelligence artificielle qui tend à mieux définir et encadrer le recours à de telles pratiques en observant toujours le risque encouru[1268].

432. Une occultation de données supplémentaires au cas par cas – Il incombe aux parties de demander l'occultation de données supplémentaires. Aussi, le juge peut décider de lui-même d'occulter certaines données dont la diffusion est susceptible de porter atteinte à la sécurité ou au respect de la vie privée des individus. L'occultation peut alors concerner les données identifiantes des parties à la procédure mais aussi des tiers, magistrats et greffiers. Les coordonnées de l'autorité auprès de laquelle déposer ces demandes d'occultations supplémentaires doivent être fournies sur le portail de diffusion. Cette décision relève du président de la formation de jugement ou du magistrat qui a pris la décision s'agissant des demandes déposées par les parties ou tiers à la procédure, et par le président de la juridiction quand la demande émane d'un magistrat ou d'un greffier[1269]. S'agissant de la question de « l'anonymisation » des données permettant l'identification des juges et greffiers intervenant dans la décision, le décret du 29 juin 2020 ne prévoit pas une occultation de principe mais une occultation au cas par cas s'il existe un risque pour leur sécurité ou leur vie privée.

433. Mise à disposition électronique sécurisée – Au vu du système existant et des normes européennes, se pose la question de la protection des données contenues dans les décisions mises à disposition comme le prévoit la loi du 23 mars 2019. La première garantie apportée par le décret d'application en date du 29 juin 2020 résulte de son article 7 qui prévoit que la mise à disposition des décisions se fait via un portail placé sous la responsabilité du ministre de la justice[1270].

La diffusion et la mise à disposition des décisions de justice sont donc encadrées en ce qui concerne la publicité des données à caractère personnel contenues dans celle-ci. Passée la mise en œuvre de la publicité se pose la question du sort des données ayant fait l'objet d'un fichage au cours de la procédure.

[1268] Commission Européenne, livre blanc sur l'intelligence artificielle – une approche européenne axées sur l'excellence et la confiance, 19 février 2020, COM 2020 65 final.
[1269] Art. R.111-12 du code de l'organisation judiciaire. Voir, N. Fricero, Open data des avocats : comment garantir les droits fondamentaux des parties ?, *Procédures,* n 10, octobre 2020, et. 23.
[1270] Art. R111-10 du code de l'organisation judiciaire.

Section 2 : La gestion des données à caractère personnel fichées

434. Gestion des données – Il s'agit ici de s'interroger sur les modalités et les normes encadrant la gestion des données à caractère personnel qui font l'objet au cours d'une procédure judiciaire d'un fichage au sein d'un fichier judiciaire[1271]. Les textes portant création de fichiers fixent leurs modalités de gestion dans le respect des normes législatives en vigueur. Aussi, le règlement général sur la protection des données, la directive « Police-Justice » et la loi informatique et libertés ont réaffirmé et renforcé les droits des personnes visées par un traitement de données. Il s'agit dans un premier temps d'observer les normes encadrant la gestion des données à caractère personnel fichées (§1.), puis ensuite de s'intéresser aux droits des individus quant à la gestion de leurs données (§2.).

§1. Les normes encadrant la gestion des données à caractère personnel fichées

435. La protection des données fichées par l'encadrement de leur conservation et rectification – Il s'agit ici de s'interroger sur la protection des données à caractère personnel fichées et sur les différentes problématiques qui se posent liées notamment à l'interconnexion de fichiers soulevant de fait la question de la finalité de ces derniers. S'agissant des fichiers de police, les textes portant création du fichier fixent les modalités de gestion de ces derniers. Il convient de s'intéresser aux normes encadrant la gestion des fichiers judiciaires (A.) et plus précisément aux faits justifiant une rectification ou un effacement de droit des données fichées (B.).

A. Les normes encadrant la gestion des fichiers judiciaires

436. Gestion des fichiers – Placés sous la responsabilité d'une entité déterminée, les fichiers judiciaires sous soumis à des dispositions légales qui encadrent la durée de conservation des données (1°) qu'ils contiennent mais aussi les modalités de transfert de celles-ci (2°).

[1271] La notion de fichier de police est entendue largement est renvoie aux données fichées en cours de procédure ou aux données utilisées au cours de celle-ci est provenant de fichier judiciaires ou administratifs.

1° Les durées légales de conservation des données contenues dans les fichiers de police

437. Durées légales de conservation des données au fichier d'antécédents judiciaires (TAJ) – Sans faire une présentation exhaustive des fichiers judiciaires existants, il est intéressant d'analyser les durées de conservation de données fixées pour certains des principaux fichiers.

Par exemple s'agissant du traitement des antécédents judiciaires (TAJ) placé sous la responsabilité du ministère de l'intérieur, et qui recense notamment les données relatives aux personnes mises en cause et de victimes d'infractions, ce dernier contient grand nombre de données d'identification constituant donc des données à caractère personnel. Il s'agit d'un fichier visant à faciliter la constatation et la répression des infractions ayant donc une finalité répressive. Les données relatives aux mis en cause majeurs sont par principe conservées vingt ans[1272]. Cette durée peut être réduite à cinq ans pour certains délits ou portée à quarante ans pour des infractions criminelles. Les données du mis en cause mineur sont, elles, conservées cinq ans, durée qui peut être portée à dix ans en matière de vol ou violences par exemple ou à vingt ans pour certains crimes. Ce fichier contient aussi des données relatives aux victimes. Elles sont conservées quinze ans avec possibilité d'en demander l'effacement dès lors que l'auteur des faits a été condamné de manière définitive. Enfin, le fichier a aussi vocation à conserver les données relatives aux individus pour lesquels la cause de la mort est suspecte et inconnue ou relatives aux personnes disparues. Dans ce cas, les données sont conservées jusqu'à la résolution de l'enquête, ce qui apparait en lien avec la finalité du fichier.

438. Durées légales de conservation des données au FIJAIS – Le FIJAIS a vocation à conserver des données relatives aux individus ayant commis des infractions violentes ou sexuelles. La finalité réside dans la lutte contre la récidive et l'identification des suspects. Peuvent faire l'objet d'un fichage au FIJAIS les individus mis en examen, les individus condamnés pour les infractions cités avant même que la décision ne soit devenue définitive, même en cas de dispense de peine, et les individus pour lesquels une composition pénale a été ordonnée. Aussi, la personne reconnue comme irresponsable pour cause de trouble mental peut figurer au fichier. Les données sont conservées trente ans pour les crimes et délits punis de dix ans d'emprisonnement et vingt ans dans les autres cas à compter de l'inscription au

[1272] Art. R.40-27 du code de procédure pénale.

fichier ou à compter de la libération si une peine d'emprisonnement ferme est effectuée[1273]. S'agissant des mineurs de treize ans ou plus, les données sont conservées dix ans.

439. Durées légales de conservation des données au FNAEG – Le FNAEG est un fichier d'identification conservant les traces ADN dans le but notamment de permettre une identification future d'auteurs d'infractions. Il conserve donc des données identifiantes dont des données génétiques. Au vu de la finalité du fichier et de la nature des données conservées, la durée de conservation est fonction du statut de l'individu concerné, du motif d'inscription au fichier et de la nature de l'infraction en cause. La durée de conservation peut aller jusqu'à quarante ans s'agissant de personnes condamnées, ou ayant fait l'objet d'une enquête quant bien même celle-ci aurait été classée sans suite ou pour lesquelles un non-lieu a été prononcé[1274]. Les données conservées dans le but retrouver une personne disparue ou d'identifier une personne décédée sont conservées jusqu'à ce que la personne ait été retrouvée ou identifiée ou à défaut quarante ans. Les données relatives aux individus mis en cause sont conservées vingt-cinq ans. Ces données sont issues soit de traces biologiques non rattachées à une identité, soit de prélèvements d'échantillons réalisés sur des individus en matière d'infractions visées à l'article 706-55 du code de procédure pénale[1275].

440. Durées légales de conservation des données au FIJAIT – Le FIJAIT a été créé dans le but de prévenir la commission d'infractions à caractère terroristes et de faciliter l'identification des auteurs. La durée de conservation des données dépend du motif ayant

[1273] Art. 706-53-4 du code de procédure pénale.
[1274] Art. R53-14 du code de procédure pénale.
[1275] Art. R53-10 du code de procédure pénale. L'article 706-55 du code de procédure pénale vise « 1° Les infractions de nature sexuelle visées à l'article 706-47 du présent code ainsi que le délit prévu par l'article 222-32 du code pénal ;
2° Les crimes contre l'humanité et les crimes et délits d'atteintes volontaires à la vie de la personne, de torture et actes de barbarie, de violences volontaires, de menaces d'atteintes aux personnes, de trafic de stupéfiants, d'atteintes aux libertés de la personne, de traite des êtres humains, de proxénétisme, d'exploitation de la mendicité et de mise en péril des mineurs, prévus par les articles 221-1 à 221-5, 222-1 à 222-18, 222-34 à 222-40, 224-1 à 224-8, 225-4-1 à 225-4-4, 225-5 à 225-10, 225-12-1 à 225-12-3, 225-12-5 à 225-12-7 et 227-18 à 227-21 du code pénal ;
3° Les crimes et délits de vols, d'extorsions, d'escroqueries, de destructions, de dégradations, de détériorations et de menaces d'atteintes aux biens prévus par les articles 311-1 à 311-13, 312-1 à 312-9, 313-2 et 322-1 à 322-14 du code pénal ;
4° Les atteintes aux intérêts fondamentaux de la Nation, les actes de terrorisme, la fausse monnaie, l'association de malfaiteurs et les crimes et délits de guerre prévus par les articles 410-1 à 413-12, 421-1 à 421-6,442-1 à 442-5, 450-1 et 461-1 à 461-31 du code pénal ;
5° Les délits prévus aux articles 222-52 à 222-59 du code pénal, aux articles L. 2339-2, L. 2339-3, L. 2339-4, L. 2339-4-1, L. 2339-10 à L. 2339-11-2, L. 2353-4 et L. 2353-13 du code de la défense et aux articles L. 317-1-1 à L. 317-9 du code de la sécurité intérieure ;
6° Les infractions de recel ou de blanchiment du produit de l'une des infractions mentionnées aux 1° à 5°, prévues par les articles 321-1 à 321-7 et 324-1 à 324-6 du code pénal. »

entrainé l'inscription. La personne poursuivie pour des faits de terrorisme est inscrite au fichier pour une durée de vingt ans ramenée à dix pour les mineurs. Cette durée est de cinq ans quant l'inscription relève d'une violation d'une interdiction de sortie du territoire ou de violation d'un contrôle administratif, ramenée à trois ans pour les mineurs[1276].

2° Les normes régissant le transfert des données fichées

441. Le potentiel transfert de données fichées après le procès – Après clôture de la procédure et avant l'effacement des données contenues dans les fichiers judiciaires se pose la question d'un éventuel transfert de celle-ci qui pourrait, de fait, prolonger leur durée de conservation. Sans revenir sur les modalités de ces éventuels transferts et leurs conséquences, il s'agit davantage de s'interroger sur les conséquences en termes de protection des droits des individus s'agissant de données issues d'une procédure achevée. La Commission nationale de l'informatique et des libertés a, à des nombreuses reprises, tiré la sonnette d'alarme s'agissant des risques encourus du fait du transfert des données personnelles d'un fichier à l'autre. En termes de protection des droits des individus, il faut s'interroger sur les conséquences de la multiplication des interconnexions de fichiers entre eux, sur l'extension de leurs finalités pour certains et sur le développement d'applications permettant un rapprochement ou une consultation des données fichées. La loi informatique et libertés prévoit par exemple que les demandes d'avis relatifs aux traitements qui présentées à la CNIL fassent état des éventuelles interconnexions et rapprochements[1277]. De plus, le journal des opérations tenu par le responsable du traitement doit mentionner les éventuels transferts de données ou interconnexions[1278]. Le traitement de données relatives aux infractions est licite à la condition d'être nécessaire. Les autorités sont autorisées à traiter des données sensibles au sens de l'article 6 de la loi informatique et libertés en cas de « nécessité absolue »[1279]. La loi informatique et libertés vise donc bien le traitement nécessaire au vu de la finalité de la mission des autorités. C'est là que se pose la question des données transférées d'un fichier à l'autre. Le législateur entend toutefois limiter cette extension de finalité potentielle en prévoyant que les données collectées 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 menaces pour la sécurité publique et la prévention de telles

[1276] Art. 706-25-6 du code de procédure pénale.
[1277] Art. 33 de la loi informatiques et libertés.
[1278] Art. 101 de la loi informatiques et libertés.
[1279] Art. 88 de la loi informatique et libertés.

menaces »[1280] , ne peuvent faire l'objet d'un traitement pour une autre finalité sans qu'un texte vienne le prévoir strictement[1281]. Cette extension doit elle aussi répondre au critère de nécessité du traitement[1282]. Aussi, si les données sont soumises à des conditions de traitement spécifiques, l'autorité qui transmet ces données doit en avertir le destinataire[1283].

La loi informatique et libertés prévoit également la possibilité de recourir à des sous-traitants. Ces derniers doivent apporter des « garanties suffisantes » quant aux droits des personnes concernées par le traitement[1284]. Cette relation est encadrée par un acte juridique qui définit outre la finalité du traitement, les obligations en termes de sécurité à mettre en œuvre et la durée de ce traitement[1285].

De manière générale, le responsable de traitement ou le sous-traitant ont une obligation de contrôle sur l'exactitude des données traitées et doivent si nécessaire opérer des rectifications ou effacements[1286]. Finalement, le responsable du traitement doit assurer « un niveau de protection adapté au risque »[1287]. La nature des données contenues dans les fichiers judiciaires et leur potentiel transfert vers d'autres fichiers constituent évidemment un risque pour celles-ci. En cela, le responsable doit s'assurer que seules les personnes habilitées aient accès aux données et que celles-ci sont traitées de manière sécurisée notamment lors de leurs éventuels transferts[1288]. Ces dispositions peuvent néanmoins soulever des interrogations quant à leur possible mise en œuvre dans la pratique. La tenue d'un journal des opérations qui relate toutes les actions effectuées sur les données, de la simple consultation à la modification, permet de savoir en théorie qui a accédé aux données et aussi de connaitre les éventuels transferts et interconnexions dont elles ont fait l'objet[1289].

Faisant là encore le choix d'une responsabilisation des acteurs du traitement, le législateur a, dans la loi informatique et libertés, rappelé les obligations incombant au responsable. Ainsi, sur la question de la gestion des données fichées, il appartient au responsable de s'assurer à la fois de la mise à jour de celles-ci et dans le cas de transfert de l'information des destinataires. De plus, les interconnexions qui auraient pour conséquence d'étendre la finalité initiales des données collectées doivent être encadrées par un texte nouveau prévoyant les dispositions

[1280] Art. 87 de la loi informatique et libertés.
[1281] Art. 91 de la loi informatique et libertés.
[1282] Art. 92 de la loi informatique et libertés.
[1283] Art. 91 de la loi informatique et libertés.
[1284] Art. 96 de la loi informatique et libertés.
[1285] *Ibid*.
[1286] Art. 97 de la loi informatique et libertés.
[1287] Art. 99 de la loi informatique et libertés.
[1288] *Ibid*.
[1289] Art. 101 de la loi informatique et libertés.

précises propres à ce nouveau traitement. Il peut néanmoins dans la pratique apparaitre compliqué d'assurer un tel traçage des données.

B. Les faits justifiant une rectification ou un effacement de droit des données fichées

442. Rectification et effacement des données fichées – Certains faits justifient une rectification ou un effacement des données fichées. Il faut donc distinguer les cas dans lesquels cette rectification ou cet effacement est automatique, des requêtes qui peuvent être présentées par les individus concernées. Cet effacement peut être automatique et fondé sur le critère de finalité (1°), ou relever d'une nécessaire mise à jour (2°).

1° L'effacement d'office fondé sur le critère de finalité du traitement

443. L'effacement d'office sur critère de nécessité – Il s'agit ici de s'intéresser à ce que Céline de Terwangne nomme « le droit à l'effacement au sens large »[1290] qui découle des normes européennes et renvoie au principe de finalité du traitement. L'auteure fait référence à la « conséquence automatique », par laquelle en principe l'individu obtient « sans effort » l'effacement des données[1291]. L'article 17 du règlement général sur la protection des données vise « un droit d'obtenir du responsable l'effacement des données ». Ce critère de finalité et de nécessité du traitement justifie notamment de ne pouvoir obtenir l'effacement de données en cours de procédure et constitue une limite au droit d'effacement. Le règlement général sur la protection des données vise à l'article 17 §1 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 ». Par principe, le responsable du traitement, en l'occurrence le procureur de la République, qui, s'agissant des fichiers de police, doit s'assurer de l'exactitude des données fichées et de leur nécessité, doit d'office faire procéder à cet effacement. Ce motif peut également fonder une requête en effacement déposée par l'individu concerné.

[1290] C. de Terwangne, « Droit à l'oubli, droit à l'effacement ou droit au déréférencement ? Quand le législateur et le juge européens dessinent les contours du droit à l'oubli numérique », *in Enjeux européens et mondiaux de la protection des données personnelles* (sous la dir. de A. GROSJEAN), Bruxelles, Larcier, 2016. Ce « droit à l'effacement au sens large » complète le « droit à l'effacement stricto sensu » découlant des dispositions de l'article 17 §1 d) du règlement général sur la protection des données qui renvoie au droit à l'effacement des données pour illicéité du traitement reprenant ainsi les dispositions de la directive du 24 octobre 1995.
[1291] C. de Terwangne, « Droit à l'oubli, droit à l'effacement ou droit au déréférencement ? Quand le législateur et le juge européens dessinent les contours du droit à l'oubli numérique », *op. cit.*

444. L'effacement d'office sur le critère de faits justificatifs – D'autres faits ont pour conséquence l'effacement automatique des données. Par exemple s'agissant des données conservées dans le FIJAIS, l'article 706-53-4 du code de procédure pénale précise que celles-ci sont effacées au décès de la personne. Toutefois, les dispositions précisent également que l'amnistie, la réhabilitation ou l'effacement des mentions au casier judiciaire national n'entraine pas l'effacement des données au fichier. S'agissant du fichier d'antécédents judiciaires, l'article 230-8 du code de procédure pénale dispose que le procureur de la République compétent peut d'office opérer l'effacement des données notamment en cas de requalification judiciaire. Aussi, par principe, les données sont effacées en cas de relaxe ou d'acquittement exception faite des cas où le procureur de la République décide du maintien.

De plus, par principe, les données conservées dans les fichiers d'analyse sérielle sont effacées notamment dans le cas d'enquête pour recherche des causes de la mort lorsque celle-ci a permis d'écarter tout crime ou délit, ou de la même manière, lorsque le fichage intervient dans le cadre d'une enquête en recherche d'une personne disparue et que celle-ci est retrouvée[1292]. Dans tous ces cas, l'effacement des données au fichier est par principe effectué d'office sauf exception, et repose sur le fait qu'au vu de la finalité du traitement la conservation n'est plus nécessaire. On peut ici rejoindre le raisonnement précédent selon lequel cet effacement peut être réalisé d'office par le responsable du traitement ce qui n'empêche néanmoins pas une requête émanant de la personne visée par le traitement sur le fondement plus général des motifs visés à l'article 17 du règlement général ou par la loi informatique et libertés.

On peut également citer le traitement de pré-plainte en ligne mis en œuvre par décret du 24 mai 2018[1293]. Ce dispositif permet aux justiciables de signaler des faits constitutifs d'infractions dans le but d'une éventuelle procédure. Ces derniers renseignent des données personnelles liées notamment à leur identité et aux faits. Cette déclaration est alors transmise aux services de police et de gendarmerie. Les données ainsi collectées sont effacées à la signature de la plainte où à défaut trente jours après la déclaration en ligne[1294].

[1292] Art. 230-15 du code de procédure pénale.

[1293] Décret n° 2018-388 du 24 mai 2018 relatif au traitement automatisé de données à caractère personnel dénommé « pré-plainte en ligne ».

[1294] Décret n° 2018-388 du 24 mai 2018 relatif au traitement automatisé de données à caractère personnel dénommé « pré-plainte en ligne », art. 4.

2° La mise à jour des données fichées

445. La rectification automatique des données – Il s'agit ici des cas dans lesquels une rectification de droit est opérée sur les données du fichier. S'agissant des fichiers d'antécédents par exemple, l'article 230-8 du code de procédure pénale dispose qu'en cas de requalification judiciaire, la rectification est de droit. Le procureur de la République compétent peut alors d'office demander la rectification ou l'effacement des données au fichier. L'article 4 de la loi informatique et libertés dispose que les données faisant l'objet d'un traitement doivent être « exactes » et « si nécessaire tenues à jour », ce qui suppose une mise à jour en temps réel.

446. La mise à jour par l'interconnexion entre fichiers – Les données fichées doivent faire l'objet de mises à jour afin de refléter, en temps réel, la situation de l'individu concerné. Cette mise à jour a fait l'objet de nombreuses critiques émises sur le fichier STIC notamment auquel il était reproché de contenir beaucoup d'erreurs et de n'être pas mis à jour régulièrement. Aujourd'hui remplacé par le traitement des antécédents judiciaires, résultat de sa fusion avec le JUDEX[1295], le fichier est interconnecté à l'application de la chaine pénale Cassiopée. Cette interconnexion avec l'outil de saisi et de suivi des affaires pénales, qui est pour l'heure au stade de l'expérimentation, semble sur ce point[1296] permettre une réelle mise à jour du traitement d'antécédents.
De telles rectifications peuvent également résulter d'une action de l'individu concerné par le traitement par l'exercice de ses droits.

§2. Les droits des individus quant à la gestion de leurs données à caractère personnel fichées

447. Droits reconnus sous l'influence des normes européennes – Le législateur a rappelé dans les lois récentes l'existence pour les individus de droits quant à la gestion des données qui les concernent. S'agissant des données traitées au cours de procédures judiciaires, ces droits renvoient notamment au droit à être informé de tout traitement le concernant, du droit

[1295] V. *supra* n°161 s.
[1296] Il a pu être à de nombreuses reprises soulevé le fait que l'interconnexion si elle permet une meilleure mise à jour du fichier pour l'avenir ne résoudra pas le problème des erreurs contenues dans les anciennes fiches reprises au STIC et JUDEX. Supra

d'accès et de rectification des données traitées et enfin du droit d'opposition et d'effacement de ces données. Il s'agit donc ici de s'interroger sur les droits dévolus aux individus qui leurs permettent de demander à ce qu'une action particulière soit exercée sur leurs données. Le droit à l'effacement sera abordé dans le second paragraphe relatif à l'oubli. Cela passe avant tout par l'attribution d'un droit d'accès. L'absence de droit d'opposition au traitement de données en matière judiciaire (A.), ne prive néanmoins pas les individus d'un droit d'accès aux données fichées lors de procédures judiciaires (B.) et soulève la question des sanctions pour non respect des droit des individus (C.).

A. L'absence de droit d'opposition au traitement de données en matière judiciaire

448. L'exception au droit d'opposition – L'article 21 du règlement général sur la protection des données prévoit un droit d'opposition au traitement des données à caractère personnel. Ce droit permet dans certains cas et pour certains motifs ayant trait à la « situation particulière » de l'individu, de s'opposer à ce que ses données fassent l'objet d'un traitement. Dans ces cas, le responsable du traitement doit cesser le traitement des données sauf s'il invoque des motifs « légitimes et impérieux » qui prévalent alors. Les dispositions de l'article 21 du règlement général sur la protection des données visent les données traitées à des fins de prospection, ou à des fins scientifiques, statistiques ou historiques. Elles visent également les traitements nécessaires à l'exécution d'une mission d'intérêt public[1297], les traitements relevant d'intérêts légitimes[1298], qui constituent des bases légales de traitement de données. Le traitement de données basé sur une mission d'intérêt public vise de manière générale celui mis en œuvre par une autorité publique dans le but de réaliser ses fonctions. Il ressort dans un premier temps de ces dispositions l'application du droit d'opposition aux traitements mis en œuvre par les autorités judiciaires dans le cadre de leurs missions. Toutefois, l'article 110 de la loi informatique et libertés précise que si toute personne peut s'opposer au traitement des données personnelles qui la concernent, ce droit ne s'applique pas lorsque le traitement découle d'une obligation légale ou qu'il est écarté par les textes.

Le droit d'opposition bien que visant grand nombre de traitements de données à caractère personnel ne s'applique pas aux traitements mis en œuvre par les autorités judiciaires et administratives s'agissant notamment des fichiers judiciaires et de renseignement, le fichage

[1297] Tels que visés à l'article 6 §1 e) du règlement général sur la protection des données.
[1298] Tels que visés à l'article 6 §1 f) du règlement général sur la protection des données.

dans ces fichiers relevant de dispositions légales, ce qui au demeurant découle d'une évidence au vu de la finalité des fichiers.
On peut néanmoins citer les dispositions de l'article R40-33 qui prévoient s'agissant du TAJ la possibilité pour les victimes de s'opposer à la conservation des données qui les concernent dès lors que l'auteur des faits est condamné par un jugement définitif.
Cette quasi absence de droit d'opposition en matière de fichiers judiciaires n'exclue néanmoins pas l'application des autres droits dont dispose les personnes.

B. Le droit d'accès aux données fichées lors de procédures judiciaires

449. Le droit d'accès préalable nécessaire à l'exercice des ses droits – L'exercice de droits sur les traitements de ses données à caractère personnel suppose au préalable d'avoir connaissance de ces traitements. Il convient de s'interroger sur l'étendue du droit d'accès (1°) pour comprendre l'application faite aux données contenues dans les fichiers judiciaires (2°).

1° L'étendue du droit d'accès

450. Finalités du droit d'accès – La mise en œuvre des droits déterminés par le règlement général sur la protection des données et la loi informatique et libertés suppose dans un premier temps la possibilité d'accéder aux données. Ce droit défini à l'article 15 du règlement général sur la protection des données permet à tout individu de savoir si des données personnelles le concernant font ou non l'objet d'un traitement. Il s'exerce, par principe, auprès du responsable du traitement. L'exercice de ce droit permet de connaitre la finalité du traitement, la nature des données traitées, les destinataires de ces données et toutes les personnes susceptibles d'en avoir connaissance et la durée de conservation[1299]. Aussi, l'individu faisant jouer son droit d'accès doit être informé du droit de rectification, d'effacement, de limitation du traitement et d'opposition dont il dispose[1300]. En cela, le droit d'accès constitue la première étape dans l'exercice des autres droits à la disposition des individus. Aussi, au vu des dispositions de l'article 15 du règlement général, l'individu doit être informé de la source des données lorsque celles-ci ne sont pas collectées directement auprès de lui.
Au sein de la loi informatique et libertés, ce droit d'accès est évoqué à l'article 49 qui renvoie pour son application aux dispositions du règlement général sur la protection des données.

[1299] Art. 15 du Règlement général sur la protection des données.
[1300] *Ibid*.

Aussi, s'agissant plus spécifiquement des traitements relatifs aux infractions, l'article 105 de la loi informatique et libertés reprend les dispositions de l'article 15 du règlement général sur la protection des données quant à l'étendue de ce droit. L'article 107 de la loi informatique et libertés apporte une première limitation à l'application de ces dispositions en prévoyant notamment une possible restriction des droits de la personne lorsque les données sont traitées au cours d'enquêtes, de mise à exécution de sanctions pénales ou lorsque cela est nécessaire à la protection de la sécurité publique ou nationale par exemple. De plus, l'article 111 de la loi informatique et libertés précise que les dispositions des articles 104 et suivants de celle-ci, relatifs aux droits de la personne, ne s'appliquent pas s'agissant des données collectées au cours de procédures judiciaires en matière pénale. Dans ce cas, l'accès aux données et les conditions de rectification et d'effacement relèvent des dispositions du code de procédure pénale. Si le droit d'accès a une portée générale permettant à tout individu visé par un traitement de données à caractère personnel d'avoir connaissance de ce traitement, sa mise en œuvre diffère en fonction de la nature du traitement en question. C'est notamment le cas s'agissant des fichiers judiciaires.

2° L'application du droit d'accès aux données contenues dans les fichiers judiciaires

451. Le système dual d'accès aux données fichées –Dans son application, il faut distinguer deux procédures s'agissant du droit d'accès aux données. Si par principe ce droit s'exerce de manière directe auprès du responsable, certains traitements ne sont accessibles qu'indirectement. Il convient donc de distinguer les cas où l'accès aux données fichées est direct (a°), des cas où il est indirect (b.).

a° L'accès direct aux données fichées

452. Le principe de l'accès direct auprès du responsable du traitement – Le décret du 1er aout 2018 pris pour application de la loi informatique et libertés modifiée par la loi du 20 juin 2018[1301] est venu modifier les dispositions relatives à l'accès au traitement des antécédents judiciaires (TAJ). Dès lors, le droit d'accès au fichier se fait directement auprès du ministère de l'intérieur, responsable du traitement[1302]. Là encore, ce droit peut faire l'objet de restrictions.

[1301] Loi 2018-493 du 20 juin 2018 relative à la protection des données personnelles.
[1302] Art. R40-33 du code de procédure pénale.

S'agissant des données alimentant le système d'information Schengen (SIS II), l'exercice du droit d'accès s'exerce auprès du ministère de l'intérieur responsable du traitement lorsqu'il s'agit de données relatives à l'état civil, le sexe, la nationalité, les photographies ou de manière générale lorsqu'elles concernent les objets volés[1303]. Le fichier des personnes recherchées est placé sous la responsabilité du ministre de l'intérieur, le droit d'accès s'exerce, de fait, également auprès du ministère.
En ce qui concerne l'accès aux données du fichier national des empreintes génétiques et du fichier national des empreintes digitales, le droit d'accès s'exerce auprès du service central de police technique et scientifique qui en est responsable.

453. L'exception à l'accès indirect en raison de la nature des données – L'exercice du droit d'accès aux données fichées peut être direct par dérogation au principe d'accès indirect en raison notamment de la nature des données visées. C'est le cas par exemple s'agissant du système d'information Schengen (SIS II). L'article R231-12 du code de la sécurité intérieure dispose que le droit d'accès aux données fichées s'exerce, par principe, auprès de la Commission nationale de l'informatique et des libertés. La dérogation prévue s'agissant de certaines données telles que l'identité laisse supposer que c'est la nature des données fichées qui justifie l'exercice indirect des droits.

b° L'accès indirect aux données fichées

454. Le principe d'un accès indirect aux données en raison de la nature du traitement – Par principe l'accès aux données des fichiers de renseignements relevant de la direction générale de la sécurité intérieure, de la direction générale de la sécurité extérieure ou de la direction du renseignement et de la sécurité de la défense, se fait de manière indirecte auprès de la CNIL. Cet accès est indirect en raison de la nature des données traitées et cette nature justifie également que l'accès puisse être restreint. Aussi, le responsable peut décider de ne pas communiquer toutes les données en raison de la finalité du traitement. Dans ces cas, les demandes doivent être déposées auprès de la CNIL et sont traitées par un magistrat de la Commission. Ces dispositions ne visent pas, en soi, l'accès à un fichier judiciaire mais cette précision permet à la fois un parallèle avec les fichiers administratifs et de plus la porosité entre les deux peut justifier de s'interroger sur l'accès à ces derniers.

[1303] Art. R231-12 du code de la sécurité intérieure.

455. L'accès indirect aux données en raison des restrictions légales – Le droit d'accès aux données fichées peut, par dérogation, faire l'objet de restrictions fixées par la loi. Par exemple, s'agissant du traitement des antécédents judiciaires (TAJ), l'article R40-33 du code de procédure pénale prévoit par dérogation, que l'accès peut être restreint notamment afin de prévenir toute entrave à des enquêtes ou procédures judiciaires[1304], renvoyant ainsi aux dispositions de l'article 107 de la loi informatique et libertés.

De manière plus générale, le droit d'accès aux données peut s'exercer de manière indirecte en cas d'opposition par le responsable ou d'absence de réponse dans les deux mois qui suivent la demande. Le droit d'accès ne s'exerce alors pas auprès du responsable du traitement. Par exemple, s'agissant du traitement des antécédents judiciaires (TAJ) ou du fichier des personnes recherchées (FPR), en cas d'opposition ou d'absence de réponse, l'individu peut exercer son droit devant la CNIL. Il peut également saisir le tribunal administratif contre la décision de restriction.

456. L'exercice du droit de rectification des données à caractère personnel faisant l'objet d'un traitement – Par l'exercice du droit d'accès au traitement de ses données, tout individu peut en demander la rectification s'il constate une erreur. L'exercice de ce droit renvoie donc au raisonnement précédent concernant le droit d'accès et fait application de l'article 4 de la loi informatique et libertés qui dispose que les données traitées doivent être actualisées. Là aussi, le constat est celui d'une rectification d'office par le responsable du fichier des données qui ne seraient plus exactes. Néanmoins, la personne visée peut exercer son droit de rectification si elle constate une erreur. Par exemple, concernant les données fichées au TAJ, la demande de rectification doit, à peine d'irrecevabilité, être adressée au procureur de la République par lettre recommandée avec accusé de réception[1305]. En cas de refus opposé, le demandeur peut dans un délai d'un mois saisir le président de la chambre de l'instruction ou le président de la chambre de l'instruction de la Cour d'appel de Paris et doit motiver sa demande[1306]. De la même manière le demandeur peut agir en cas d'absence de réponse par le procureur de la République[1307].

L'exercice de ces droits est encadré et garantie par la condamnation de leur non respect.

[1304] Art. R40-33 III du code de procédure pénale.
[1305] Art. 40-31 du code de procédure pénale.
[1306] Art. 40-31-1 du code de procédure pénale.
[1307] *Ibid*.

C. Les sanctions du non respect des droits des individus quant au traitement de leurs données à caractère personnel

457. Pouvoirs de sanction de la CNIL – La méconnaissance des droits accordés aux individus quant au traitement de leurs données peut faire l'objet de sanctions émanant soit de la Commission nationale de l'informatique et des libertés (1°) soit du juge au regard du droit pénal (2°).

1° Le pouvoir de sanction de la CNIL

458. Dispositions générales – La CNIL a vu ses pouvoirs en termes de contrôle a posteriori et de sanctions accroitre suite à l'entrée en vigueur du règlement général sur la protection des données et l'adoption de la loi informatique et libertés dans sa nouvelle rédaction[1308]. L'affirmation et l'accentuation de cette fonction répressive constitue une contrepartie à l'allégement de ses missions en termes d'autorisation aux traitements de données. Ainsi, du fait d'une plainte déposée auprès d'elle ou d'un contrôle, la Commission peut prononcer des mesures visant la mise en conformité avec les normes internes et européennes. Il peut donc s'agir d'un simple rappel à l'ordre, d'une injonction de mise en conformité du traitement, d'une suspension temporaire ou permanente de celui-ci, d'un retrait de certification, d'une suspension des flux de données ou d'une amende administrative. Cette dernière est encadrée par les dispositions de l'article 83 du règlement général sur la protection des données qui fixe un plafond de 20 000 000 d'euros ou 4% du chiffre d'affaires mondial de l'exercice précédent, s'agissant d'entreprises. A titre d'exemple et sans que cela ne concerne directement l'exercice du droit d'accès à des données fichées au sein d'un fichier judiciaire, la CNIL a, dans une délibération en date du 18 mai 2017, prononcé une sanction pécuniaire de 10 000 euros à l'encontre d'une société pour méconnaissance du droit d'accès. Aussi le 10 octobre 2019, la Commission a prononcé une sanction pécuniaire et une injonction sous astreinte à l'encontre d'une société pour non respect du droit d'accès et d'effacement et défaut de confidentialité des données[1309].

459. La réalité du contrôle a postériori relatif à l'exercice des droits des personnes s'agissant des fichiers judiciaires – Avant de s'interroger sur le contrôle opéré par la CNIL

[1308] Art. 8 de la loi informatique et libertés.
[1309] Rapport annuel d'activité CNIL 2019, p.92.

en termes de respect des droits des personnes quant au traitement de leurs données s'agissant des fichiers judiciaires il convient de s'intéresser à la réalité de ce contrôle. Le développement exponentiel du nombre de fichiers couplé au fait que les individus sont désormais mieux renseignés sur leurs droits a entrainé une explosion du nombre de demandes d'accès, de rectification ou d'effacement des données contenues dans les fichiers de police. Le rapport d'activité édité par la CNIL pour l'année 2019 fait état de 14137 plaintes contre 11077 en 2018 soit une hausse de 27 %. La Commission a prononcé en 2019, huit sanctions dont une seule pour méconnaissance du droit d'accès[1310]. Cette même année, 300 contrôles ont été effectués par les 215 agents que compte la Commission avec un budget alloué de 18,5 millions d'euros[1311]. Ce constat permet dans un premier temps de s'interroger sur les moyens alloués à la CNIL afin de remplir ses missions[1312] notamment au vu de l'augmentation de ses missions de contrôle a posteriori.

S'agissant des contrôles opérés sur les fichiers judiciaires, le rapport de 2019 fait d'abord état d'une certaine confusion quant au mode d'action des individus, certains saisissant directement la CNIL alors qu'il s'agit d'un droit d'accès direct, notamment s'agissant des fichiers relavant de la directive « Police-Justice ». Néanmoins la CNIL reste compétente pour faire jouer son droit d'accès indirect en cas d'absence de réponse par le responsable du fichier judiciaire. En 2019, sur la totalité des saisines 1% concernait le fichier Cristina, 2% le FPR et 11% le TAJ[1313]. Ces dernières n'ayant donné lieu à aucune sanction.

2° La méconnaissance des droits des individus constitutive d'infractions pénales

460. Dispositions du code pénal – La méconnaissance des droits posés par les normes européennes et internes constituent une infraction pénale. Ainsi, l'article 40 de la loi informatique et libertés renvoie aux dispositions du code pénal. De manière générale, l'article 226-16 du code pénal prévoit l'incrimination liée au « 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 ». L'article

[1310] Rapport annuel d'activité CNIL 2019, p.81.
[1311] *Ibid*., p.111.
[1312] V. Gautron, *Fichiers de police, réglementation française*, Répertoire de droit pénal et de procédure pénale, *op. cit*., 40-42. L'auteure analysait alors les chiffres de 2013 en comparaison notamment à ceux de 2000. En 2013 le budget de la CNIL s'élevait à 16,9 millions d'euros et ses effectifs à 178 agents traitant cette année là 5640 plaintes. La comparaison avec les précédents bilans amenait l'auteure à conclure en un manque de moyens alloués à la Commission « entravant » de fait « l'effectivité des contrôles ». Ce constat semble d'autant plus vrai aujourd'hui au vu des chiffres exposés dans le rapport de 2019 et notamment du nombre exponentiel de plaintes.
[1313] Rapport annuel d'activité CNIL 2019, p.86.

R625-11 du code pénal dispose, notamment, que le fait de ne pas informer une personne qui en fait la demande de ce que ses données personnelles font ou non l'objet d'un traitement, de ne pas l'informer sur la nature des données traitées ou la finalité du traitement est constitutif une contravention de cinquième classe. Constitue une contravention de cinquième classe la méconnaissance des droits des personnes s'agissant du traitement de leurs données à caractère personnel sauf restrictions légales[1314]. Est constitutif d'une même infraction le fait de méconnaitre les droits de rectification, de mise à jour et d'effacement[1315].

La gestion des données collectées au cours d'une procédure judiciaire renvoie aux interventions exercées d'office par le responsable du traitement et à l'exercice par les individus de leurs droits. Parmi ces droits, figure le droit à l'effacement qui trouve à s'appliquer de manière particulière s'agissant des données fichées en matière judiciaire. Celui-ci renvoie directement à la notion d'oubli et justifie son étude au sein d'une partie consacrée de manière plus générale à l'oubli en matière judiciaire.

[1314] Art. 107, Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.
[1315] Art. R625-12 du code pénal.

CHAPITRE 2 : LE DROIT A L'OUBLI DES DONNEES A CARACTERE PERSONNEL COLLECTEES DANS LE CADRE D'UNE PROCEDURE JUDICIAIRE

461. Précisions terminologiques – La question appelle nécessairement des précisions terminologiques préalables. De la définition du droit à l'oubli dépend le raisonnement qui en découle en termes de traitement de données. Le premier constat assez simple est celui qui consiste à définir le droit à l'oubli comme une prérogative offerte aux individus permettant que certaines données les concernant soient oubliées[1316]. L'oubli peut se définir comme « l'effacement, la disparition des souvenirs » ou encore comme la « disparition de la mémoire collective d'un groupe »[1317]. Sans aller plus loin dans l'analyse terminologique, se dessinent déjà plusieurs pistes de réflexions. Il convient donc de s'interroger sur la notion même de droit à l'oubli afin d'en mesurer la portée notamment en termes de données à caractère personnel traitées lors de procédures judiciaires. En partant d'interrogations pourtant simples, on mesure à quel point cette notion est diffuse. Il convient alors de s'interroger sur l'objet de l'oubli, sur la temporalité de sa mise en œuvre ou encore sur les débiteurs du droit. La première interrogation vise à comprendre l'étendue de ce droit. La seconde permet de fixer l'émergence du « droit à » et enfin la dernière permet d'identifier les individus débiteurs de ce droit. Enfin il faut s'interroger sur les modalités de mise en œuvre de ce droit qui révèle *de facto* ses limites. Ce droit se trouve évidemment confronté notamment à la mémoire et au droit à l'information ou à la liberté d'expression. En s'interrogeant sur l'évolution de la notion même de « droit à l'oubli » et sur sa reconnaissance tant jurisprudentielle, doctrinale que législative, on comprend que ce droit n'est pas absolu. Ainsi, on a pu assister à l'émergence de la notion de droit à l'oubli puis à la reconnaissance d'un droit à l'effacement des données (Sect.1). Il convient de s'interroger sur l'effectivité du droit à l'oubli s'agissant des données à caractère personnel intervenant dans les procédures judiciaires (Sect.2).

[1316] Voir en ce sens, Boizard M. (dir.), Blandin A., Corgas C, Dedessus Le Moustier G., Gambs S., Lejealle C, Moisdon-Chataigner S., Pierre P.,Piolle G., Rousvoal L., *Le droit à l'oubli*, Mission de recherche Droit et Justice, févr. 2015, p. 13. http://www.gip-recherche-justice.fr/publication/le-droit-loubli-2/

[1317] Dictionnaire Larousse

Section 1 : De l'émergence du droit à l'oubli à la reconnaissance d'un droit à l'effacement des données

462. Problématique – La première question qui se pose est celle de l'existence réelle d'un droit à l'oubli. La réponse dépend nécessairement de la définition retenue de l'oubli et de ce qu'on entend par droit à l'oubli. L'étude de la notion même de droit à l'oubli permet de s'apercevoir de l'évolution de celle-ci. Cette évolution est sans aucun doute le fruit des évolutions technologiques et de communication. Le développement d'internet et du *big data* ont conduit à repenser le concept de droit à l'oubli qui s'avère aujourd'hui plus proche d'un droit à l'effacement, ces deux notions n'étant pas similaires. Ainsi, il s'agit dans un premier temps de s'interroger sur la reconnaissance progressive d'un droit à l'oubli (§1.) puis dans un second temps sur son application aux données traitées au cours des procédures judiciaires (§2.).

§1. La reconnaissance progressive d'un droit à l'oubli

463. Le droit à l'oubli une notion fluctuante – La reconnaissance d'un droit à l'oubli est le résultat d'un processus jurisprudentiel, doctrinal et législatif progressif marqué par des avancées et des retours en arrière[1318]. L'étude de ces différents processus témoigne de l'évolution qui entoure le concept même de droit à l'oubli. Avant d'être reconnu comme une notion à part entière, l'essence du droit à l'oubli a pu être dégagé de certaines décisions sans pour autant que le juge n'y fasse strictement référence. Toutefois, si le législateur semble avoir pris récemment le parti de qualifier ce droit, la comparaison avec la jurisprudence ou la doctrine antérieure laisse penser que ce dernier a finalement enfermé l'oubli dans un carcan plus restreint. Il convient dans un premier temps de s'interroger sur la notion même de droit à l'oubli, cette définition permettant d'en appréhender la portée. Cette réflexion apparait nécessaire à l'étude plus spécifique de l'oubli relatif aux données traitées lors de procédures

[1318] On peut brièvement citer l'affaire dite « Landru » jugée le 14 octobre 1965 (TGI Seine, 14 octobre 1965, *JCP* 1966 I 14482). La requérante demandait réparation d'un préjudice lié à la réalisation d'un film relatant une affaire criminelle. Les juges civils faisant référence à une « prescription du silence » avaient toutefois rejeté sa demande notamment parce que cette dernière avait elle-même publié ses mémoires relatant l'affaire et que de plus le film ne reprenait que des faits mentionnés dans la décision librement accessible. L'affaire est intéressante notamment par l'étude ces commentaires qui en ont été fait. C'est à cette occasion que le professeur Gérard Lyon-Caen fait pour la première fois référence au droit à l'oubli. Commentant la décision du 14 octobre 1965, il pose le droit à l'oubli comme fondement à l'action de la requérante. Cette décision esquisse les modalités de mise en œuvre de l'oubli. En effet, le fait que le requérant diffuse lui-même l'information est aujourd'hui encore admis comme motivant le rejet d'une telle demande.

judiciaires. Il convient donc de s'intéresser à cette reconnaissance jurisprudentielle du droit à l'oubli (A.) afin d'observer sa consécration (B.).

A. La reconnaissance jurisprudentielle du droit à l'oubli

464. Le « droit à l'oubli », une notion développée par doctrine – L'idée d'un droit à l'oubli s'agissant de données traitées en matière judiciaire est née d'un raisonnement doctrinal, puis a fait l'objet d'une consécration jurisprudentielle. Il convient de s'intéresser à l'émergence de la notion d'oubli dans le droit (1°) et à sa consécration jurisprudentielle (2°).

1° L'émergence de la notion d'oubli dans le droit

465. Précisions terminologiques – Le terme d'oubli renvoie évidemment à celui de mémoire. Il peut être défini comme « l'effacement, la disparition des souvenirs »[1319] ou encore comme la « disparition de la mémoire collective d'un groupe »[1320]. La notion de « droit à l'oubli » renverrait donc à l'idée d'une créance détenue par les individus leur permettant d'obtenir que les données les concernant soient oubliées. Ce droit subjectif supposerait donc qu'il prime sur d'autres droits et principes et que les individus disposent de prérogatives leur permettant d'atteindre cet objectif. Il s'agira plus tard de s'interroger sur l'existence réelle d'un « droit à » l'oubli, en tant que droit subjectif.

466. L'oubli dans les lois encadrant l'amnistie – La notion d'oubli se retrouve en premier lieu dans les textes encadrant l'amnistie par exemple. L'amnistie peut être définie comme « le processus d'oubli volontaire qui conduit le législateur à reconsidérer régulièrement les faits et les actes réalisés pour leur ôter pour l'avenir la coloration pénale qu'il pouvaient avoir »[1321].

467. L'oubli par la réhabilitation – La réhabilitation a pu être présentée comme la « technique d'effacement la plus exigeante »[1322]. La réhabilitation qu'elle soit légale ou judiciaire permet de ne plus se voir opposer la décision prononcée à son encontre et renvoie

[1319] Dictionnaire Larousse
[1320] *Ibid*.
[1321] B. Py, *Amnistie*, Répertoire de droit pénal et de procédure pénale, octobre 2003, actualisation juin 2012.
[1322] M. Herzog-Evans, *Réhabilitation*, Répertoire de droit pénal et de procédure pénale, avril 2008, actualisation mars 2018.

donc à une forme de pardon qui repose sur l'oubli de la condamnation[1323]. Ce mécanisme suppose de rassembler plusieurs conditions et notamment une condition de temps. En cela, ces procédés sont évidemment attachés à l'oubli, accordant à l'individu concerné de ne plus se voir opposé son passé judiciaire et imposant donc d'une certaine manière l'oubli de celui-ci. Il s'agit ici d'une présentation succincte permettant de comprendre l'émergence de « l'oubli » dans le droit. Ces procédés de réhabilitation ou d'amnistie seront abordés plus loin s'agissant de leurs conséquences.

2° La reconnaissance jurisprudentielle du droit à l'oubli

468. L'émergence d'un droit à l'oubli fondé sur l'existence d'un préjudice et sur le critère temporel – Dans une décision du 20 avril 1983, le tribunal de grande instance de Paris a jugé que « toute personne qui a été mêlée à des évènements publics peut, le temps passant, revendiquer le droit à l'oubli ; que le rappel de ces évènements et du rôle qu'elle a pu y jouer est illégitime s'il n'est pas fondé sur les nécessités de l'histoire ou s'il peut être de nature à blesser sa sensibilité » ajoutant que ce droit s'applique à tous et s'impose à tout le monde[1324]. Le droit à l'oubli semble alors attaché au critère temporel et sur l'atteinte que pourrait causer le fait de rappeler les faits. Ainsi, pendant longtemps l'oubli ne renvoyait pas à un principe mais plus à un concept applicable au cas par cas. Par exemple, dans une décision du 20 novembre 1990 relative à la parution d'un livre relatant une affaire pénale jugée, la Cour de cassation a précisé que les condamnations pénales ne relevaient pas du domaine de la vie privée, laissant planer un flou sur les fondements permettant d'invoquer un potentiel droit à l'oubli s'agissant de condamnations anciennes[1325]. Si dans la décision du 20 avril 1983 le droit à l'oubli justifiait que soit interdite la rediffusion d'une affaire ancienne, force est de constater que par la suite ce droit semble avoir un temps été oublié lui-même[1326]. L'idée d'un droit à l'oubli se trouve attaché au critère temporel. L'oubli est lié au concept de prescription qui impose, passé un certain délai, d'oublier les faits[1327]. Néanmoins, le développement du numérique et des bases de données informatiques ont conduit à repenser ce droit à l'oubli.

[1323] Art.133-12 du code pénal s'agissant de la réhabilitation légale et article 782 du code pénal s'agissant de la réhabilitation judiciaire.
[1324] TGI Paris, 20 avril 1983, *JCP G*, 1983. II. 20434.
[1325] Cass., civ. 1ère, 20 novembre 1990, *pourvoi* n° 89-12.580.
[1326] T. Hassier, Droit de la personnalité, *Dalloz*, 2007, 2829.
[1327] La prescription a pu être qualifiée de « grande loi de l'oubli ».

469. L'oubli dirigé par l'atteinte à la vie privée – Si la notion de droit à l'oubli est d'abord apparue en matière de responsabilité civile, puis s'est développée en matière pénale sur le fondement de l'atteinte au droit au respect de la vie privée conséquence du fait de relater d'anciens faits relatifs à une affaire pénale ancienne.

Néanmoins en la matière la jurisprudence a pu être fluctuante. Par exemple dans l'arrêt de la Cour européenne des droits de l'Homme, *Fuchsmann c/ Allemagne* du 19 octobre 2017[1328], la Cour européenne a considéré que le droit à l'information primait sur l'oubli. Il s'agissait en l'espèce d'une demande de retrait d'un article de presse en ligne relatant les faits d'une enquête pénale pour laquelle les poursuites avaient finalement été abandonnées. Les requérants invoquaient le fait que l'article étant toujours accessible celui-ci portait atteinte à leur vie privée. Sur le fondement de l'intérêt public à disposer de ces données, la Cour européenne des droits de l'homme a considéré que le droit à l'information primait[1329]. S'agissant d'un livre faisant référence à une condamnation, la Cour de cassation a même, par le passé, considéré que les données relatives aux condamnations ne relevaient pas de la vie privée[1330]. Aujourd'hui plus nuancée, la Cour de cassation admet qu'il puisse y avoir une atteinte au droit au respect de la vie privée qui trouve toutefois ses limites dans le droit à l'information du public[1331].

Parfois présentée comme une consécration européenne, le règlement général sur la protection des données fait directement référence au droit à l'oubli. Cette reconnaissance est toutefois discutable.

B. La reconnaissance d'un droit à l'oubli numérique par l'affirmation du droit à l'effacement de données pour motifs légitimes

470. Du droit à l'oubli numérique au droit à l'effacement de données – Bien que le règlement général sur la protection des données fasse référence au « droit à l'oubli », il faut s'interroger sur son existence réelle. Dans un premier temps, on observe l'émergence d'un droit à l'oubli numérique (1°), puis la reconnaissance d'un droit au déréférencement (2°) et enfin la consécration d'un droit à l'effacement des données pour motifs légitimes par le droit européen (3°).

[1328] Cour E.D.H., *Fuchsmann c/ Allemagne, 19 octobre 2017, req. n°71233/13.*
[1329] On pourrait néanmoins s'interroger en l'espèce sur l'atteinte potentielle à la présomption d'innocence.
[1330] Cass., civ. 1ère, 20 novembre 1990, JCP 1992. II. 21908.
[1331] Par exemple en matière de presse, Cass., civ. 1ère, 12 mai 2016, *pourvoi* n°15-17.729.

1° L'émergence d'un droit à l'oubli numérique

471. Le nécessaire encadrement des données numériques – Le développement du numérique et le *big data* ont donné une nouvelle dimension aux questions relatives à la gestion des données à caractère personnel. Naturellement, le droit à l'oubli s'est trouvé dirigé sur des préoccupations davantage numériques engageant de fait un virage dans la définition même qui en est faite. L'émergence des notions « d'identité numérique »[1332] ou de « réputation numérique » marquent cette évolution. Dans son rapport d'activité de 2013, la Commission nationale de l'informatique et des libertés vise « la possibilité offerte à chacun de maîtriser ses traces numériques et sa vie en ligne, qu'elle soit privée ou publique »[1333]. Dans un rapport d'information en date du 8 octobre 2015, la Commission de réflexion et de proposition sur « le droit et les libertés à l'âge du numérique » suggérait que soit consacré un « droit à l'autodétermination informationnelle donnant sens aux droits reconnus à l'individu sur les réseaux numériques »[1334]. Le règlement général sur la protection des données a nécessairement orienté le droit à l'oubli en fonction des évolutions du numérique, mais force est de constater qu'il l'a enfermé dans le carcan des durées de conservation des données[1335]. La doctrine a pu rappeler que le droit à l'oubli tel que développé antérieurement renvoie à une notion pourtant bien distincte du droit à l'effacement. En effet, le droit à l'oubli est en réalité plus large que le droit d'effacement. Le second étant finalement un outil nécessaire à l'obtention du premier[1336]. Sur la base d'une réflexion engagée en 2009 a été rédigée une charte relative au droit à l'oubli numérique. Cette dernière, a été signée le 13 octobre 2011 par grand nombre des représentants des moteurs de recherche ou sites collaboratifs qui s'engageaient à faciliter la mise en œuvre des droits des individus s'agissant de leurs données personnelles mises en ligne. Néanmoins il était alors regrettable que certains d'entres eux tels que Google ou Facebook n'y aient pas adhéré. Cette charte s'inscrit dans le mouvement qui tend à vouloir, dans certains domaines, développer davantage le *soft law* permettant en amont que soit mises en œuvre des « bonnes pratiques » et facilitant ainsi le respect des règles[1337].

[1332] Avec notamment la création du délit d'usurpation d'identité numérique par la loi 2011-267 du 14 mars 2011.
[1333] Rapport d'activité annuel de la CNIL, 2013.
[1334] Rapport n° 3119 de la CNIL, 8 octobre 2015, recommandation 58.
[1335] M. Boizard, Le temps, le droit à l'oubli et le droit à l'effacement, *Les cahiers de la justice*, 2016, p. 619.
[1336] *Ibid*.
[1337] S. Guicherd, M.L. Caron-Fasan, N. Lesca, Droit à l'oubli numérique : quel alignement entre chartes et pratiques ?, in Dechenaud David, *Le droit à l'oubli numérique, données nominatives, approches comparée*, Larcier, 2014.

472. Une première reconnaissance s'agissant des données numériques des mineurs – En 2001, la Commission nationale de l'informatique et des libertés a rendu un avis relatif à la collecte de données personnelles des mineurs sur internet. Face au développement du numérique, d'internet et des réseaux sociaux notamment, il est apparu nécessaire d'accorder une protection renforcée s'agissant des données relatives aux mineurs.

Initialement, les textes encadrant le traitement des données à caractère personnel ne comprenaient pas de dispositions particulières s'agissant des mineurs. L'idée d'une protection renforcée à leur égard a été émise dans un avis du groupe de travail G29 en date du 11 février 2009[1338]. Dans cet avis, le groupe de travail s'est intéressé aux traitements de données portant sur les mineurs et notamment en milieu scolaire pour évaluer la pertinence de la protection apportée à ces données au vu de la minorité du public concerné et des normes relatives aux droits des enfants.

Dans cet optique d'apporter une protection spécifique aux mineurs, le législateur a, dans la loi pour une République numérique du 7 octobre 2016, consacré un droit à l'oubli spécifique aux mineurs, leur permettant de demander l'effacement des données les concernant collectées alors qu'ils étaient mineurs. Cette action peut être engagée peu importe que l'individu soit mineur ou majeur du moment que la collecte de données ait, elle, eu lieu lors de la minorité. Ces dispositions ont été reprises dans la loi informatique et libertés[1339]. Le règlement général sur la protection des données contient également des dispositions particulières attachées à la minorité du public concerné par le traitement. Toutefois, il ne fait pas référence aux mineurs mais vise les « enfants ». Ainsi, l'article 8 du règlement général relatif au consentement des mineurs s'agissant des services d'information, dispose que les traitements dont la licéité est attachée au consentement de l'individu concerné s'applique aux enfants d'au moins seize ans. Si un tel traitement vise un mineur de moins de seize ans, le consentement doit être donné par son représentant légal. Les dispositions du texte prévoient que les Etats sont libres de fixer un âge inférieur dans la limite des treize ans. Le règlement général dispose également qu'il incombe au responsable du traitement de vérifier que le consentement a bien été donné par le titulaire de l'autorité parentale quand cela est nécessaire. Il s'agit donc là de dispositions qui enjoignent au responsable de traitement de mettre en œuvre des mesures particulières et

[1338] Avis du groupe « article 29, n°2/2009 sur la protection des données à caractère personnel de l'enfant, 11 février 2009.

[1339] Art. 51, 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.

protectrices s'agissant des données relatives aux mineurs[1340]. Cette volonté d'accorder une protection renforcée s'agissant des données à caractère personnel relatives aux mineurs a été une première étape dans la mise en œuvre de dispositions visant la protection des données numériques. Ensuite, la jurisprudence a développé un droit au déréférencement plus général.

2° La reconnaissance d'un droit au déréférencement

473. Les apports de l'arrêt *Google Spain* – De l'idée de départ d'un droit à l'oubli, s'est développée celle d'un droit à l'oubli numérique ou droit au déréférencement[1341]. Dans une décision du 13 mai 2014 *Google Spain*, la Cour de justice de l'Union européenne, distingue dans un premier temps les données faisant l'objet d'un traitement par des éditeurs et le traitement découlant des recherches sur les moteurs de recherche. Ainsi, elle affirme qu'une recherche sur un moteur de recherche à partir d'un nom, constitue bien un traitement de données au sens des normes européennes auxquelles il est donc soumis en ce qu'elle permet d'accéder à des données mises en ligne, de les indexer de manière automatique, de les stocker temporairement et de les mettre à disposition selon un ordre particulier. Aussi, les moteurs de recherche sont responsables de ces traitements. Les individus visés peuvent donc demander à ce que les données les concernant n'apparaissent plus lors d'une recherche par leur nom. Il faut toutefois bien préciser que le déréférencement ne supprime pas la base de données en elle-même mais permet que celle-ci n'apparaisse plus dans les résultats d'une recherche effectuée sur un moteur de recherche. Toutefois, ce droit se trouve mis en concurrence avec le droit à l'information du public qui peut justifier le rejet d'une demande de déréférencement. Par cette décision, la Cour de justice de l'Union européenne a consacré, avant même le règlement général sur la protection des données, une forme de droit à l'oubli « numérique ».

474. Les critères d'appréciation d'une demande de déréférencement établis par la CNIL – La Commission nationale de l'informatique et des libertés a établi en 2014 une liste de critères visant à faciliter l'étude des plaintes relatives au déréférencement de données. Ce questionnaire livre une interprétation de la jurisprudence en la matière et a le mérite d'offrir une présentation claire et concise du droit au déréférencement et de son application en confrontant, quand cela est nécessaire, ce droit avec d'autres droits et libertés. Ainsi, sans reprendre une présentation exhaustive du questionnaire, la CNIL soulève la question de l'âge

[1340] Voir, O. Foret, Droit à l'oubli des mineurs, *Dalloz IP/IT*, 2018, p.350-352.
[1341] Encore appelé « désindexation ».

de l'individu visé par le traitement et rappelle que la minorité offre une protection quasi automatique. Aussi, la Commission rappelle que des données qui seraient inexactes, excessives ou non pertinentes peuvent motiver le déréférencement. Le critère de sensibilité des données au sens de la loi est notamment observé, puisque le traitement de données sensibles est strictement encadré, par principe, et que la diffusion de telles données peut potentiellement porter atteinte à la vie privée des personnes. Renvoyant au critère temporel, la Commission précise que si les données sont périmées ou ne sont plus d'actualité cela peut justifier leur déréférencement. De plus, même si celui-ci n'a pas à être prouvé, l'accès à des données qui causeraient un trop grand préjudice est pris en compte dans les demandes. Dans cette étude, la CNIL observe qui est à l'origine de la publication des informations en question. L'individu qui rend des données publiques y consent par principe, néanmoins il peut par la suite demander le déréférencement de celles-ci. La Commission rappelle que les demandes doivent être analysées au regard des finalités de diffusion des données. Par exemple, si les données sont diffusées à des fins de journalisme il convient de s'interroger sur le préjudice causé au requérant et d'analyser sa demande au regard, là encore, du critère temporel renvoyant ici à l'idée de la prescription. S'agissant de données publiées du fait d'une obligation légale, le déréférencement reste l'exception et résulte le plus souvent de la double condition de préjudice et de temporalité. Enfin s'agissant des données pénales, la CNIL renvoie aux dispositions légales régissant la matière et précise l'importance du critère de gravité des faits et d'ancienneté de leur commission.

475. Précisions quant à la portée du déréférencement – Il faut bien distinguer l'éditeur d'une page web contenant des données à caractère personnel et le responsable d'un moteur de recherche de part leur finalité notamment. L'éditeur peut avoir une vocation journalistique et donc ce contexte ne permet pas l'exercice du droit d'opposition ou de rectification par les individus concernés. S'agissant du moteur de recherche, ces droits peuvent être exercés. Dans une ordonnance de référé du 19 décembre 2014[1342], les juges internes ont fait une première application de la jurisprudence *Google Spain*. Ils ont considéré que le fait pour un individu de voir apparaitre sur un moteur de recherche des données relatives à une condamnation ancienne peut nuire à la personne notamment dans sa recherche d'emploi et justifie que ces données fassent l'objet d'un déréférencement.

[1342] TGI Paris, ordonnance de référé, 19 décembre 2014, M. Mme X et M. Y c/ Google France.

La Cour de justice de l'Union européenne a récemment apporté des précisions relatives au droit au déréférencement, notamment dans deux décisions du 24 septembre 2019. Dans la première décision[1343], la Cour de justice énonce que l'exploitant d'un moteur de recherche est soumis aux dispositions qui encadrent le traitement de données notamment s'agissant des données sensibles ou liées aux condamnations pénales. Au regard des atteintes que son activité peut porter aux libertés des individus et à leur vie privée, ce dernier est responsable des traitements mis en œuvre. A ce sujet, elle rappelle que l'exploitant du moteur de recherche n'est pas responsable de la page web contenant d'éventuelles données mais du lien créé entre la recherche saisie et la page en question, donc du référencement. En conséquence, la Cour de justice de l'Union européenne précise que lorsque le lien établi par le moteur de recherche mène à une page web contenant des données sensibles la demande doit être appréciée au regard des autres intérêts en jeu. L'exploitant du moteur de recherche doit s'interroger sur le caractère « strictement nécessaire » du référencement. Néanmoins, un tel traitement demeure possible en particulier si la personne a elle-même rendue ces données publiques.
La seconde décision du même jour est venue préciser la portée du droit au déréférencement affirmant qu'il n'y a pas de droit mondial au déréférencement imposé par les textes et par le règlement général notamment[1344].

3° La consécration d'un droit à l'effacement des données pour motifs légitimes par le droit européen

476. Une consécration numérique du droit à l'oubli – Au vu des évolutions attachées à la notion d'oubli s'agissant du traitement de données personnelles, il convient de s'interroger sur les réformes mises en œuvre par le législateur européen et interne en la matière. Cette notion de droit à l'oubli née dans la jurisprudence et développée par la doctrine trouve ses premières sources dans les normes européennes. L'adoption du règlement général sur la protection des données consacre, sous le spectre du droit à l'oubli, un droit à l'effacement. Ce droit vise d'un côté l'effacement légal fondé sur les durées de conservation des données fixées par les textes et de l'autre la prérogative offerte aux individus de demander l'effacement de données les concernant en invoquant des motifs particuliers. Profondément inscrit dans le mouvement législatif actuel orienté vers l'encadrement des traitements numériques, le règlement européen sur la protection des données a, dans son article 17, consacré un droit à l'effacement des

[1343] CJUE, 24 septembre 2019, C-136/17.
[1344] CJUE, 24 septembre 2014, C-507/17

données pour certains motifs définis qui a, peut être maladroitement été désigné comme « droit à l'oubli.[1345] »

477. Les dispositions de l'article 17 du RGPD – L'article 17 du règlement général sur la protection des données dispose qu'une personne concernée par un traitement de données à caractère personnel est en droit d'obtenir du responsable l'effacement de ses données. Cette démarche peut être engagée pour divers motifs, notamment, lorsque les données ne sont plus nécessaires au vue de la finalité du traitement, lorsque la personne retire son consentement, lorsqu'elle fait jouer son droit d'opposition et qu'aucun motif légitime impérieux ne permet la poursuite du traitement, ou lorsque le traitement est illicite par exemple. En outre, l'article 17 envisage le cas dans lequel le responsable du traitement a rendu les données publiques. Dans ce cas, si la personne fait jouer son droit à l'effacement des données, le responsable doit, dans la mesure du possible, alerter les autres responsables ayant traité les données en question et les informer de la demande d'effacement. Toutefois, ces dispositions ne s'appliquent pas dans certains cas précisés par l'article 17 du règlement. C'est le cas si le traitement est nécessaire à l'exercice de la liberté d'expression ou du droit à l'information, lorsqu'il s'agit d'exécuter une mission d'intérêt public, en matière de santé publique ou lorsque le traitement est mis en œuvre à des fins archivistes ou statistiques. Enfin, les dispositions précitées ne s'appliquent pas lorsque le traitement est nécessaire à la constatation, l'exercice ou la défense d'un droit en justice. S'agissant de données fichées au cours d'une procédure judiciaire au sein d'un fichier de police ou de renseignement, le droit d'effacement ou de rectification s'exerce selon les dispositions spécifiques prévues par les textes.

478. Les finalités du droit à l'effacement des données à caractère personnel faisant l'objet d'un traitement – Le droit européen et le droit interne ont consacré un droit à l'effacement des données à caractère personnel faisant l'objet d'un traitement. Ce droit a pu être défini dans la directive 95/46/CE du 24 octobre 1995 comme résultant « non seulement du fait que ces données sont inexactes, mais, en particulier, aussi du fait qu'elles sont inadéquates, non pertinentes ou excessives au regard des finalités du traitement, qu'elles ne sont pas mises à jour ou qu'elles sont conservées pendant une durée excédant celle nécessaire, à moins que leur conservation s'impose à des fins historiques, statistiques ou scientifiques ». Aussi, la loi du 6 aout 2004 transposant la directive dispose que « Toute

[1345] L'article 17 du RGPD vise dans son intitulé le « droit à l'effacement (droit à l'oubli) ».

personne physique justifiant de son identité peut exiger du responsable d'un traitement que soient, selon les cas, […] effacées les données à caractère personnel la concernant, qui sont inexactes, incomplètes, équivoques, périmées, ou dont la collecte, l'utilisation, la communication ou la conservation est interdite »[1346]. Ce droit s'exerce donc de deux manières. Soit en raison de l'inexactitude ou du manque de pertinence des données traitées, soit en raison de la durée de conservation de ces données. Cette dernière possibilité renvoie à l'idée selon laquelle les données ne peuvent pas être conservées indéfiniment ou encore si cette conservation ne va plus dans le sens de la finalité qui a justifié le traitement. Il ressort de ce constat l'idée plus générale de l'existence d'un droit à l'oubli. Ce droit à l'oubli a pris une dimension particulière du fait du développement *du big data* et en termes de données judiciaires cette question se pose d'autant plus du fait de *l'open data* judiciaire.

479. Application et portée – Toute personne concernée par un traitement de données peut donc demander au responsable du traitement l'effacement des données le concernant pour un des motifs définis par la loi, tels que la nécessité, le retrait de consentement ou par l'exercice du droit d'opposition. L'article 17 du règlement apporte des précisions sur la portée du droit d'effacement et répond, au moins sur le fond, à une interrogation qui se pose s'agissant de l'oubli sur internet. Ainsi, le texte dispose que lorsqu'une demande d'effacement est présentée au responsable d'un traitement, ce dernier doit prendre des « mesures raisonnables, y compris d'ordre technique » pour informer les autres responsables traitant ces mêmes données de la demande déposée. L'objectif étant que les copies et reproduction de données soient également effacées. Ces dispositions renvoient notamment aux questions de rediffusion des données qui constitue une des problématiques de la mise en œuvre de l'oubli s'agissant des données numériques.

Après cette présentation des différentes composantes de l'oubli et du potentiel droit à l'oubli, il convient de s'interroger plus spécifiquement sur son application s'agissant des données de procédures.

[1346] Loi 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.

§2. Le droit à l'oubli appliqué aux données traitées au cours de procédures judiciaires

480. L'oubli judiciaire – Il ressort de l'analyse précédente que la notion de droit à l'oubli est née dans la doctrine et la jurisprudence. Le législateur a préféré consacrer un droit à l'effacement des données et un droit au déréférencement. Pour reprendre l'analyse de Cécile de Terwangne, la notion de droit à l'oubli apparait finalement plus large que celle de droit à l'effacement[1347]. Le droit à l'oubli s'entend comme englobant à la fois le droit à l'effacement des données et le droit au déréférencement[1348], bien qu'il semble plus large encore. L'oubli peut donc être rattaché au critère de temps (A.) ou découler de l'application de critères protecteurs des droits des individus (B.).

A. L'oubli attaché au critère de temps

481. Dualité de l'oubli judiciaire – Le droit à l'oubli s'agissant des données à caractère personnel traitées lors de procédures judiciaires peut résulter de l'application de textes encadrant soit leur durée de conservation et imposant donc leur effacement sur un critère temporel, ou par l'application de textes qui sur le fondement de motifs particuliers imposent cet « oubli », renvoyant en la matière aux durées de conservation. S'agissant des données à caractère personnel faisant l'objet d'un traitement au cours de procédures judiciaires, l'oubli renvoie à cette double vocation. Ainsi, « l'oubli » peut être rattaché aux règles de prescription ou être la conséquence des normes encadrant les durées de conservation des données au sein des fichiers judiciaires.

482. L'oubli et la conservation de données – La question de l'oubli s'agissant de données intervenant dans les procédures judiciaires renvoie notamment à celle des durées de conservation s'appliquant aux données fichées. Sans revenir sur le sujet de la gestion des

[1347] C. de Terwangne, « Droit à l'oubli, droit à l'effacement ou droit au déréférencement ? Quand le législateur et le juge européens dessinent les contours du droit à l'oubli numérique », *op. cit.*, p.273-274. Pour l'auteure, le droit à l'oubli comprend « le droit au repentir et à changer d'avis à l'égard de ce que l'on a diffusé auparavant ou accepté que l'on fasse avec ses données ; le droit de ne pas voir en permanence rappelé son passé, de ne pas voir son passé encombrer le présent et hypothéquer l'avenir ; le droit d'obtenir qu'une personne ne conserve plus ce qu'elle savait parce que ce n'est plus légitime, le principe de finalité ne le justifiant plus ou parce que c'est non conforme aux règles de protection des données ; le droit de refuser la décontextualisation des données en luttant principalement contre la puissance des moteurs de recherche sur Internet, tout en admettant éventuellement que les données demeurent dans leur contexte initial ».

[1348] *Ibid.*

fichiers de police et sur la présentation de ces durées, il s'agit ici de s'interroger de manière plus globale sur l'application de ce critère temporel en termes de droit à l'oubli. Si chaque texte qui porte création d'un fichier de police en fixe les modalités de gestion et les durées maximales de conservation des données, le constat a pu être fait d'une absence d'homogénéité dans ces durées[1349]. Les positions du Conseil constitutionnel en la matière témoignent également de cette hétérogénéité[1350]. Par exemple saisi d'une question prioritaire de constitutionnalité relative au fichier national des empreintes génétiques, le Conseil constitutionnel a émis une réserve d'interprétation s'agissant des articles 706-54 et 706-55 du code de procédure pénale estimant qu'il était nécessaire de « moduler » les durées de conservation en fonction notamment de la gravité de l'infraction commise et en adaptant ces durées en cas de minorité de l'individu[1351].

Le droit européen a également une influence en la matière. S'agissant de la conservation des données génétiques au sein du FNAEG, la Cour européenne des droits de l'homme a dans un arrêt *Aycaguer c/ France* du 22 juin 2017[1352], considéré que les dispositions internes méconnaissaient le droit européen en ce qu'elles ne permettaient pas aux personnes mises en cause de demander l'effacement de leurs données et au vu de la durée légale de conservation fixée, portait de fait atteinte à l'article 8 de la Convention européenne des droits de l'homme. Désormais, les dispositions de l'article 706-54-1 du code de procédure pénale prévoit la possibilité pour les personnes fichées à la suite d'une condamnation de demander l'effacement de leurs données. Cette demande reste soumise à l'appréciation du procureur de la République compétent notamment sur le critère de nécessité ou non de conservation. Les durées de conservation réglementaires restent néanmoins hétérogènes. Si les durées fixées semblent tenir compte du statut de l'individu et de la gravité de l'infraction c'est davantage une comparaison entre fichiers qui révèle des différences de durées. Pour exemple, dans le cas d'une personne condamnée, les données génétiques et les données digitales ne seront pas conservées pendant la même durée quant bien même la finalité des deux fichiers visés

[1349] Rapport d'information de la commission des lois constitutionnelles, de la législation et de l'administration générale de la République sur les fichiers mis à la disposition des forces de sécurité, Députés PARIS D. et MOREL-A-L'HUISSIER P., op. cit.
M. Boizard, Le temps, le droit à l'oubli et le droit à l'effacement, *op. cit*.
[1350] Rapport d'information de la commission des lois constitutionnelles, de la législation et de l'administration générale de la République sur les fichiers mis à la disposition des forces de sécurité, Députés PARIS D. et MOREL-A-L'HUISSIER P., op. cit.
[1351] Cons. Const., n°2010-25 QPC, 16 septembre 2010. Suite au prononcé de ces réserves d'interprétation aucun décret n'a pour l'instant été adopté.
[1352] Cour E.D.H., 22 juillet 2017, *Aycaguer c/ France*, req. n°8806/12.

(FNAEG et FAED) est la même[1353]. Néanmoins, cette hétérogénéité témoigne aussi de la complexité qui entoure la gestion de ces fichiers. Une analyse complète nécessiterait de raisonner en prenant en compte la finalité, certes, mais aussi les modalités d'accès au fichier, leur interconnexion avec d'autres. L'utilisation concrète qui est faite du fichier et sa perméabilité peut impacter la durée de conservation initiale et réglementaire fixée. Cette multitude de critères entraine sans aucun doute un système complexe et difficile à homogénéiser en tout cas s'agissant des cadres légaux de gestion[1354].
A côté des durées légales de conservation des données, l'oubli se déduit également des principes protecteurs pour les individus.

B. L'oubli comme principe protecteur des droits des individus

483. Protection par l'oubli – L'oubli peut également s'entendre comme résultant de principes protecteurs pour les individus autres que les règles encadrant la conservation des données. Notamment il peut être la conséquence de l'orientation des poursuites qui imposent alors d'effacer les données (1°) ou de requêtes en effacement anticipé des données fichées (2°).

1° L'oubli découlant de l'issue des poursuites

484. L'oubli justifié au vu de la finalité du fichage – Au cours des procédures judiciaires, l'oubli peut être la conséquence de l'orientation des poursuites ou de l'issue du procès. Par exemple, s'agissant du traitement des antécédents judiciaires, l'article 230-8 du code de procédure pénale dispose qu'en cas de décision de relaxe ou d'acquittement définitive, les données sont effacées sauf si le procureur de la République décide de leur maintien. Au contraire, en cas de non-lieu ou de classement sans suite, les données sont inscrites au fichier sauf si le procureur de la République décide l'inverse. Ce mécanisme apparait approprié au vu de la finalité même du fichage. Une affaire jugée dans laquelle l'individu est, à l'issue de la procédure, acquitté ou relaxé justifie que celui-ci soit oublié du fichier. A contrario, une affaire classée sans suite par exemple pour manque d'éléments permettant la poursuite ou tout autre motif de classement sans suite peut justifier que les données soit un temps conservées et

[1353] Cette durée est de quarante ans s'agissant du FNAEG et de vingt-cinq s'agissant du FEAD. Voir respectivement art. R53-14 du code de procédure pénale et Art. 5 du décret du 2 décembre 2015.
[1354] Néanmoins, les droits des individus sur le traitement de leurs données appelaient une nécessaire homogénéisation. *Supra* n°

ne bénéficient pas de cet effacement « anticipé ». Cette procédure relève davantage de la gestion des fichiers et du pouvoir d'office du procureur de la République responsable du traitement[1355].

2° Les requêtes en effacement anticipé des données fichées

485. Un droit à l'effacement des données fichées conventionnellement reconnu – Le droit à l'effacement de ses données personnelles traitées n'est donc pas récent. Toutefois, force est de constater que les dispositions de la directive du 24 octobre 1995, aujourd'hui abrogée, et de la loi informatique et libertés dans sa rédaction initiale n'étaient plus adaptées au contexte actuel. En matière de droit d'effacement des données fichées l'arrêt de la Cour européenne des droits de l'homme du 18 septembre 2014 *Brunet c/ France*[1356], a apporté des précisions et rappelé la protection conventionnelle de ce droit. En l'espèce, le requérant demandait au procureur de la République compétent l'effacement de ses données du STIC à la suite d'un classement sans suite de l'affaire. Sa demande rejetée, la Cour européenne des droits de l'homme a considéré que la conservation des données était disproportionnée et portait une atteinte excessive au droit au respect de la privée. L'arrêt rappelle donc que la conservation des données à caractère personnel doit répondre à un critère de nécessité ce qui n'était en l'espèce pas le cas[1357]. Dans cette lignée, la Cour de cassation a affirmée l'existence d'un droit à l'oubli s'agissant des dispense de peine, ce qui sera ensuite consacrée par la loi du 20 juin 2018[1358] en s'appuyant sur les critères de nécessité et de proportionnalité du fichage et aussi en invoquant le fait que l'absence de communication des réquisitions ne permettait pas de mesurer de gravité des faits et donc d'apprécier le caractère nécessaire et proportionnel[1359].

486. L'effacement anticipé des données du casier judiciaire national – Lors d'un jugement en matière pénale, il est possible de demander lors de l'audience à ce que la condamnation n'apparaisse pas dans les bulletins n° 2 et 3[1360]. Cette demande peut également être faite après l'audience auprès du procureur de la République est doit être motivée par des préoccupations liées à la réinsertion de la personne notamment. Toutefois, la gravité des faits justifie

[1355] V. *supra* n°482.
[1356] Cour E.D.H., *Brunet c/ France*, 18 septembre 2014, 201010/10.
[1357] Voir, A.S. Chavent-Leclère, Rétroactivité du droit à l'effacement du fichier de traitement d'antécédents judiciaires, *Revue procédures*, n°8-9, aout 2018, comm.263.
[1358] Loi 2018-493 du 20 juin 2018 relative à la protection des données personnelles.
[1359] Cass. crim., 19 juin 2018, *pourvoi* n°16-87.749. A.S. Chavent-Leclère, Rétroactivité du droit à l'effacement du fichier de traitement d'antécédents judiciaires. *Op.cit*.
[1360] Art. 775-1 du code de procédure pénale.

l'exclusion de cette démarche comme en matière de meurtre ou assassinat commis avec torture ou actes de barbarie, proxénétisme ou prostitution de mineurs, agression sexuelle ou viol. L'effacement des mentions au bulletin n°1 relève de la procédure de réhabilitation[1361].

487. L'effacement anticipé des données du fichier d'antécédents judiciaires – Après censure du Conseil constitutionnel s'agissant des dispositions de l'article 230-8 du code de procédure pénale, il désormais possible de déposer une requête en effacement des données de fichiers d'antécédents judiciaires hors cas de classement sans suite, relaxe ou acquittement[1362]. Toutefois, cette requête doit répondre à la condition préalable que le bulletin n°2 du casier judiciaire national ne contienne aucune mention. Cette requête déposée auprès du procureur de la République vise soit l'effacement des données au fichier, soit l'apposition d'une mention visant à empêcher la consultation des données notamment dans le cadre d'enquêtes administratives.

488. L'effacement anticipé des données du FIJAIS – Quand la conservation des données ne semble plus « nécessaire compte tenu de la finalité du fichier »[1363], toute personne concernée par un fichage au FIJAIS peut demander l'effacement de ses données auprès du procureur de la République de la juridiction ayant prononcé la décision à l'origine de la mention. Toutefois, cette procédure n'est possible que si la personne a bénéficié d'une mesure de réhabilitation. De plus, aucune procédure ne doit être en cours. Enfin, l'effacement du fichier nécessite au préalable que les données aient été effacées du bulletin n°1 du casier judiciaire national[1364]. En cas de rejet de la demande ou d'absence de réponse, un recours est possible devant le juge des libertés et de la détention puis en cas de nouveau refus ou absence de réponse devant de président de la chambre de l'instruction.

489. L'effacement anticipé des données du FNAEG – Les données d'identification génétiques contenues dans le FNAEG peuvent faire l'objet d'une demande d'effacement anticipé présentée par l'individu concerné. La requête doit être déposée auprès du procureur

[1361] Art. 798 du code de procédure pénale.
[1362] Cons. Const. 2 octobre 2017, n°2017-670 QPC. N. Jacquinot, Le Conseil constitutionnel et le droit à l'oubli en matière de fichiers de police, *JCP Générale*, n°5, 29 janvier 2018, 110. B. De Lamy, Encadrement constitutionnel des fichiers de police : pas de droit à l'oubli mais un doit à demande l'effacement, *RSC*, 2018, p.993. Pour une approche plus globale, voir, N. Le Bonniec, Vers une convergence des exigences constitutionnelles et européennes en matière de protection des données personnelles numériques ?, *JCP G*, n°23, 4 juin 2018, doctr.655.
[1363] Art. 706-53-10 du code de procédure pénale.
[1364] *Ibid*.

de la République du domicile du requérant ou de la juridiction où il a été mis en cause[1365]. La décision de rejet ou l'absence de réponse dans les trois mois ouvre droit à un recours devant le juge des libertés et de la détention dont la décision peut être contestée devant le président de la chambre de l'instruction[1366]. Pour revenir sur l'arrêt de la Cour européenne des droits de l'Homme *Aycaguer c/ France* du 22 juin 2017[1367], les dispositions encadrant le droit à l'effacement des données génétiques ont fait l'objet d'une modification permettant aux personnes mises en cause de déposer une telle requête, cette dernière étant avant cela réservée aux suspects. L'article 706-54-1 du code de procédure pénale dispose que les individus condamnés faisant l'objet d'une fiche au FNAEG peuvent, après écoulement d'un délai fixé par décret, demander l'effacement de leurs données. Le procureur de la République, compétent en la matière, peut décider de l'effacement s'il estime que la conservation des données n'est plus nécessaire au vue de la finalité du fichier.

490. L'effacement anticipé des données du FIJAIT – L'effacement des données du FIJAIT peut être demandé que l'individu soit mis en examen ou condamné. La requête doit être déposée auprès du procureur de la République qui a pris la décision à l'origine de l'inscription au fichier. L'absence de réponse, passé un délai de trois mois ou le rejet de la demande peuvent faire l'objet d'un premier recours devant le juge des libertés et de la détention, décision qui peut elle-même être contestée devant le président de la chambre de l'instruction[1368]. La demande est instruite en prenant en compte, notamment, la gravité des faits, l'âge de l'individu et sa personnalité[1369].

Si l'oubli peut être la conséquence des normes encadrant la gestion des données fichées ou découlant des droits affirmés dont dispose l'individu sur le traitement des données qui le concerne, peut-on pour autant parler d'un réel droit à l'oubli en tant que droit subjectif ? Il convient donc de s'interroger sur l'effectivité de ce droit au vu de toutes les normes applicables en la matière.

[1365] Art.53-13-1 du code de procédure pénale.
[1366] Art.706.54-1 du code de procédure pénale. La loi du 23 2019 de réforme de la justice est venue créer ces dispositions afin d'aligner les voies de recours relatives au FNAEG sur celles du FIJAIS. Art.53-13-2 du code de procédure pénale.
[1367] Cour E.D.H., 22 juillet 2017, *Aycaguer c/ France*, req. n°8806/12, *op. cit.*
[1368] Art. 706-25-12 du code de procédure pénale.
[1369] *Ibid*.

Section 2 : L'effectivité du droit à l'oubli s'agissant des données à caractère personnel intervenant lors de procédures judiciaires

491. Un oubli à double dimension s'agissant des données personnelles judiciaires – De l'idée d'un droit à être oublié découlent plusieurs interrogations en termes de données judiciaires. Le sujet renvoie à deux aspects. Dans un premier temps cet oubli s'entend du droit auquel peut prétendre un individu à ce que les données qui le concernent soient oubliées par les autorités judicaires, renvoyant ici à l'effacement des fichiers de police et à la « mémoire judiciaire ». La « mémoire judiciaire » vise celle qui conserve des données à vocation judiciaire ou relatives aux condamnations aux seins de fichiers judiciaires. Dans un second temps, cet oubli s'entend comme le droit plus diffus dont disposerait un individu d'exiger que son passé judiciaire ne lui soit plus rappelé dans l'avenir, renvoyant ici à la mémoire collective. Ce droit est plus diffus car il renvoie ici à une maitrise des données notamment numériques et aux données diffusées par voie de presse dont la traçabilité demeure complexe et qui connait d'importantes limites. En définitive, l'oubli de la mémoire judiciaire vise davantage le droit à ce que les données personnelles judiciaires ne soient plus opposées aux individus. S'agissant de la mémoire collective, ce droit renvoie à l'idée plus générale d'un effacement total des données afin que la collectivité n'y accède plus, n'y fasse plus référence, ne s'en souvienne plus. Le droit à l'oubli semble dans ce second aspect complexe.

492. Oubli et mémoire judiciaire – Dans un premier temps se pose donc la question de l'effacement des données stockées au cours d'une procédure notamment au sein des différents fichiers judiciaires et au sein du casier judiciaire national, qui constitue une mémoire des condamnations. Il ne s'agit pas ici de revenir sur les durées légales qui encadrent la conservation des données au sein de ces fichiers[1370] mais plus de s'interroger sur la nécessité de conserver des données au sein de fichiers judiciaires et de s'intéresser plus spécialement au casier judiciaire national en ce qu'il constitue la « mémoire judiciaire ». Les données du casier étant accessible dans certains cas par l'administration, les données peuvent ainsi constituer des freins dans l'accès à certains emplois par exemple. En cela, l'accès aux données du casier et l'utilisation qui en est faite constitue une entrave à l'oubli dans la définition large qui peut être retenue du terme. De plus, si les données contenues dans les fichiers peuvent être effacées

[1370] V. *supra* n°136 s.

par le biais de différentes procédures, l'effacement n'est pas toujours de droit et connait des limites.

493. Oubli et mémoire collective – Ensuite, se pose la question de l'effectivité de ce « droit à l'oubli » dans la sphère collective. En pratique, l'oubli s'avère limité car confronté à des problématiques particulières. Si la gestion des données de procédures est encadrée s'agissant des données fichées, ou des données diffusées à l'issue du procès, la rediffusion de ces données notamment sur internet rend l'oubli difficile. Là aussi, le droit à l'effacement qui peut être exercé auprès des responsables de traitement s'avère limité tout comme le droit au déréférencement. Enfin, le droit à l'oubli se trouve confronté à d'autres droits et libertés.
La notion d'oubli a pu trouver différentes définitions. Si le droit européen a consacré un droit à l'effacement des données, le droit à l'oubli n'apparait pas comme un droit absolu. Le développement du numérique et de *l'open data* a conduit à repenser cette notion d'oubli. S'agissant des données traitées lors de procédures judiciaires, si les textes encadrent strictement la conservation des données et fixent les modalités d'effacement, des problématiques se posent s'agissant de la diffusion et rediffusion de données judiciaires sur internet, amenant à s'interroger sur l'effectivité d'un droit à l'oubli.
Aussi, le droit à l'effacement des données consacré au niveau européen n'est ni un droit absolu ni un droit automatique puisqu'il est attaché à des conditions de fond et reste soumis à l'appréciation du responsable du traitement.
Enfin, se pose finalement la question de l'existence réelle d'un « droit à ». L'oubli se trouve nécessairement opposé au droit à l'information ou peut céder face à un traitement qui serait nécessaire.
Il s'agit donc de s'intéresser au droit d'être oublié de la « mémoire judiciaire » (§1.), puis au droit d'être oublié de la mémoire collective (§2.).

§1. Le droit d'être oublié de la mémoire judiciaire : un droit relatif

494. Précisions terminologiques – Le terme de « mémoire judiciaire » renvoie ici aux données fichées pour les besoins d'enquêtes au sein des fichiers de police et judiciaires et notamment au sein du casier judiciaire national qui garde en mémoire les condamnations. Le constat qui ressort parfois des développements antérieurs se fonde sur la nécessaire

conservation des données au sein d'une mémoire judiciaire (A.) et sur les limites du droit à l'oubli s'agissant des données faisant l'objet d'un fichage par les autorités judiciaires (B.).

A. La nécessaire conservation des données : la mémoire judiciaire

495. Utilité des fichiers de police – L'analyse des différents fichiers judiciaires et de leurs finalités témoigne de la nécessité de constituer une mémoire des données judiciaires. Sans avoir besoin de reprendre d'exemples précis, il est évident que la constitution et l'usage des fichiers de police constitue une évolution majeure dans l'efficacité et la célérité de la résolution des affaires pénales. Evidement, ce fichage parfois massif appelle plusieurs interrogations que ce soit en termes de libertés fondamentales, de sécurité des données, mais aussi de droit à l'oubli. S'interroger sur l'effectivité d'un droit à l'oubli s'agissant des données judiciaires nécessité au préalable de s'intéresser à la nécessaire conservation des données à vocation judiciaires au sein de fichiers (1°) et au sein plus particulièrement du casier judiciaire national (2°).

1° La nécessaire conservation des données à vocation judiciaire au sein de fichiers judiciaires

496. Un fichage justifié par diverses finalités – Au cours des procédures judiciaires, la conservation de données à caractère personnel est évidemment nécessaire. Les différentes finalités des fichiers judiciaires justifient la conservation de données variées[1371]. Ainsi, les fichiers d'antécédents qui ont fusionné au sein du traitement des antécédents judiciaires (TAJ) ayant pour finalité « de faciliter la constatation des infractions à la loi pénale, le rassemblement des preuves de ces infractions et la recherche de leurs auteurs »[1372] justifient la conservation de données identifiantes et peuvent contenir des données sensibles au sens de la loi informatique et libertés[1373]. En cela, le fichier d'antécédents constitue un outil nécessaire au bon déroulement des enquêtes judiciaires. Le rapport édité par la commission des lois en 2018 fait état de 18,9 millions de fiches et plus de 87 millions d'affaires fichées au TAJ[1374].

[1371] Pour une présentation détaillée, voir, V. Gautron, *Fichiers de police, réglementation française*, Répertoire de droit pénal et de procédure pénale, *op. cit.*
[1372] Art. 230-6 du code de procédure pénale.
[1373] Art. R.40-23 et suivants du code de procédure pénale.
[1374] Rapport d'information de la commission des lois constitutionnelles, de la législation et de l'administration générale de la République sur les fichiers mis à la disposition des forces de sécurité, *op. cit.*

Les fichiers d'identification tels que le FAED, le FNAEG, le FPR ou le FIJAIS ont clairement une finalité d'identification des individus et de prévention par la conservation de données d'identification telles que les empreintes digitales ou génétiques et la conservation de traces permettant, a posteriori, l'identification d'individus. Partant d'un constat général, les différents rapports édités sur le sujet démontrent une augmentation exponentielle du nombre de fiches conservées dans les fichiers de police et judiciaires. Par exemple, le FEAD qui comptait 900 000 fiches en 1997[1375] recensait 6,2 millions de fiches en 2018[1376]. Ce constat s'applique à tous les fichiers de police et témoigne outre des évolutions législatives, des évolutions technologiques. Ainsi, les nouveaux outils à disposition des enquêteurs ont permis le recueil et la conservation de davantage de données et le législateur a, parallèlement, facilité ce recueil.

Toutefois, si le fichage peut paraitre automatique, dans certains cas il n'entraine pas pour autant une conservation des données. Par exemple, les données collectées dans le cadre d'un contrôle d'identité ne peuvent être conservées qu'en cas de suites judiciaires données à l'affaire[1377].

2° La nécessaire conservation des données relatives aux condamnations au sein du casier judiciaire national

497. Finalités du casier judiciaire national – Le casier judiciaire constitue « la mémoire judiciaire » en ce qu'il recense toutes les condamnations prononcées à l'encontre d'une personne. Organisé en bulletins qui répondent chacun à des règles de gestion, d'accès et d'apurement, différentes[1378], le casier judiciaire national qui a pour but de renseigner sur le passé judiciaire des individus constitue un outil nécessaire à l'individualisation des peines et de lutte contre la récidive. S'il répond à des règles de gestion et à des procédures d'apurement particulières, le casier judiciaire soulève des interrogations quant au possible « oubli » auquel peuvent prétendre les individus. En parallèle, se pose évidemment la question du sens de la peine mais c'est davantage la question de la nécessaire mémoire judiciaire qui trouve ici à se

[1375] Rapport du Conseil d'État, *Le numérique et les droits fondamentaux*, 2014, p.117.
[1376] Rapport d'information de la commission des lois constitutionnelles, de la législation et de l'administration générale de la République sur les fichiers mis à la disposition des forces de sécurité, *op. cit.*
[1377] Art.78-3 al . 9 du code de procédure pénale. C. Girault, *Contrôles et vérifications d'identité – Droits et garanties attachés à la rétention aux fins de vérification d'identité*, janvier 2017, Répertoire de droit pénal et de procédure pénale, actualisation mars 2018.
[1378] V. *infra* n°498.

poser[1379]. Le casier judiciaire garde en mémoire en temps réel les données relatives aux condamnations et en cela a pu être qualifié de mémoire « active »[1380]. Le bulletin n°1 du casier judiciaire est le plus complet en termes de données puisqu'il comprend toutes les condamnations et décisions de justice relatives à la personne, mais aussi certaines décisions administratives et disciplinaires, les mesures de composition pénale ou les suspensions de peine par exemple. Son accès est toutefois très restreint puisque seuls les magistrats et les services pénitentiaires peuvent le consulter. Le bulletin n°2 est accessible par certaines administrations et certaines entités privées pour des motifs précis et ne comprend que les condamnations les plus importantes exceptions faites des décisions concernant des mineurs, les décisions relatives à une déchéance d'autorité parentale ou les mesures de compositions pénales. Enfin le bulletin n°3 contient notamment les condamnations pour crimes ou délits punis d'au moins deux ans d'emprisonnement et ne peut être délivré qu'à l'intéressé.

498. Les règles d'apurement du casier judiciaire national – Les règles régissant l'effacement des données du casier judiciaire dépendent du bulletin dont il est question et de l'infraction à l'origine de l'inscription. La procédure d'effacement peut soit relever de dispositions établies par la loi et être la conséquence de certains faits, ou peut découler de l'action de la personne concernée. L'effacement du bulletin n°1 entraine par conséquent l'effacement des deux autres et l'effacement du bulletin n°2 entraine celui du bulletin n°3, témoignant donc la hiérarchie entre les trois.

Il ressort des dispositions de l'article 769 du code de procédure pénale, que les données inscrites au casier judiciaire national sont effacées après un délai de quarante ans exception faite des peines imprescriptibles. Aussi, la procédure d'amnistie ou la réhabilitation s'il elle le prévoit, entrainent l'effacement des mentions au casier. Dans les autres cas, l'effacement répond à l'écoulement d'un délai spécifique. En matière de contravention, de condamnation avec dispense de peine, de mesures éducatives, ou de composition pénale, les mentions sont retirées passées un délai de trois ans. De manière générale, le retrait des mentions au casier est subordonné à la condition qu'aucune autre condamnation ne soit intervenue entre temps. Par principe, ces mentions retirées du bulletin n°1 entrainent l'effacement des bulletins n°2 et n°3. S'agissant de l'effacement des mentions aux bulletins n°2 et n°3, celui-ci relève d'une procédure engagée par l'individu lui-même. Il peut dans un premier temps demander le jour

[1379] Pour approche plus globale, voir, M. Giocopelli, E. Gallardo, *Casier judiciaire*, Répertoire de droit pénal et de procédure pénale, septembre 2016, 10 et suivants.
[1380] *Ibid*.

de l'audience à ce que la condamnation ne soit pas inscrite au casier notamment pour des raisons professionnelles attachées à sa réinsertion. Sinon, l'effacement des mentions au casier découle d'une demande d'effacement anticipée comme en matière de fichiers de police. Toutefois ce droit est limité par plusieurs facteurs. D'abord, toutes les condamnations ne peuvent pas faire l'objet d'un retrait des bulletins n°2 et n°3 notamment s'agissant des crimes et délits graves[1381]. La demande qui doit être déposée au procureur de la République pour les condamnations relevant de sa compétence ou au procureur général pour les arrêts d'assises, doit être motivée.

Enfin, la demande de réhabilitation judiciaire favorablement accueillie entraine l'effacement du casier judiciaire[1382]. Cette procédure de réhabilitation porte sur toutes les mentions portées au casier judiciaire, elle ne peut être déposée qu'après écoulement d'un délai respectif de cinq, trois ou un an selon qu'il s'agisse d'un crime, délit ou contravention[1383]. A l'occasion d'une question prioritaire de constitutionnalité, le Conseil constitutionnel a rappelé que la procédure de réhabilitation vise à « favoriser le reclassement du condamné. Elle efface toutes les incapacités et déchéances qui résultent d'une condamnation pénale et interdit d'en rappeler l'existence à toute personne qui en a connaissance dans l'exercice de ses fonctions »[1384]. La demande de réhabilitation judiciaire fait l'objet d'une enquête. Par exemple, il faut justifier de l'accomplissement de la peine, ne pas avoir été de nouveau condamné pour des crimes ou délits et prouver une « conduite irréprochable »[1385] depuis la condamnation[1386].

De plus, la réhabilitation peut être égale et de plein-droit en ce qui concerne les peines correctionnelles et contraventionnelles passé un délai fixé par l'article 133-13 du code pénal allant de trois à dix ans en fonction de la gravité des faits. Là aussi, le but est clairement l'effacement du casier judiciaire et plus généralement la réinsertion dans la société et finalement une forme de « pardon ». Il s'agit donc bien d'une forme d'oubli qui permet à la personne condamnée, sous certaines conditions, de voir son passé judiciaire effacé en tout cas *a minima* dans les bulletins susceptibles d'être demandés par différents organismes.

[1381] Meurtre, assassinat, proxénétisme sur mineurs, agression sexuelle, viol…

[1382] Art. 798 du code de procédure pénale. L'arrêt prononçant la réhabilitation peut également prévoir le retrait de la mention au bulletin n°1. M. Giacopelli, E. Gallardo, *Casier judiciaire*, Répertoire de droit pénal et de procédure pénale, septembre 2016, *op. cit.*

[1383] Art. 785 et s. du code de procédure pénale.

[1384] Cons. const., 28 février 2020, n°2019-82 QPC, JurisData n°2020-002765. E. Bonis, Condition de recevabilité d'une demande de réhabilitation judiciaire, *Droit pénal*, n°4, avril 2020, comm.92. Le Conseil constitutionnel a été saisi sur l'appréciation des dispositions de l'article 786 du code de procédure pénale qui fixe les délais de dépôt d'une demande s'agissant d'une demande présentée après le décès du condamné par ses ayants-droits dans le cadre d'une condamnation à mort. Le Conseil constitutionnel a jugé les dispositions conformes.

[1385] Art.787 du code de procédure pénale.

[1386] M. Erzog-Evans, *Réhabilitation*, Répertoire de droit pénal et de procédure pénale, *op. cit*., 99.

Si la conservation des données à caractère personnel apparait évidemment nécessaire au bon déroulement de la justice et qu'il existe de nombreuses procédures visant l'effacement des mentions au casier, celle-ci peut néanmoins soulever des interrogations en termes d'effectivité du droit à l'oubli.

B. Les limites du droit à l'oubli s'agissant des données faisant l'objet d'un fichage par les autorités

499. Un droit encadré mais limité – Bien que strictement encadré, l'oubli n'est pour autant pas absolu s'agissant du traitement de données à caractère personnel judiciaires par les autorités. Certaines de ces limites trouvent leurs sources dans les dispositions légales elles-mêmes, d'autres sont attachées aux failles techniques de cette gestion massive de données. Il convient donc de s'intéresser aux limites du droit à l'oubli conséquences des dispositions légales encadrant la gestion des données fichées (1°), puis aux limites conséquences du traitement massif de données judiciaires (2°).

1° Les limites du droit à l'oubli conséquence des dispositions légales encadrant la gestion des données fichées

500. Un droit à l'effacement non absolu – Tout d'abord s'agissant du droit à l'effacement des données[1387] il convient d'admettre que celui-ci n'est pas absolu. Toute demande d'effacement anticipé doit être motivée ce qui laisse au procureur de la République compétent un pouvoir d'appréciation. Sur le critère de finalité de la donnée fichée et de nécessité, celui-ci peut rejeter la demande. Par exemple, l'article 230-8 du code de procédure pénale dispose que si, par principe, le fichier d'antécédents judiciaires est effacé en cas de prononcé d'une relaxe ou d'un acquittement, le procureur de la République peut décider du maintien de l'inscription au fichier s'il estime cela nécessaire, auquel cas elle fait l'objet d'une mention. Au vu de la finalité du fichier, le procureur de la République peut donc maintenir l'inscription au fichier selon un critère de nécessité.

501. Interconnexions et rapprochement de données internes – Le droit à l'oubli s'agissant des données traitées par les autorités judiciaires trouve une limite résultant de

[1387] V. *supra* n°517 s.

l'interconnexion de fichiers entre eux. Plus précisément, en partant du constat préalable de l'existence de durées de conservation très disparates d'un fichier à l'autre, on peut s'interroger sur l'application du droit à l'oubli s'agissant de données qui sont transmises d'un fichier à un autre soit par un procédé automatique soit par une recherche mettant en relation les deux[1388]. L'idée ici est qu'une donnée contenue dans un fichier de départ pour lequel une durée de conservation est fixée se retrouve fichée dans un autre avec une durée de conservation plus longue du fait d'un rapprochement de données opéré entre les deux fichiers, un fichier en alimentant un second. En cela, l'application du droit à l'oubli se trouve repoussée, par principe[1389], à la durée de conservation du second fichier[1390].

502. Interconnexion des casiers judiciaires – De manière générale se pose la question des données transférées hors du territoire et sur lesquelles ni les autorités judiciaires ni la personne concernée n'ont alors de maitrise. Plus précisément, la question trouve à se poser s'agissant du casier judiciaire européen. La création de ce « casier judiciaire européen » s'est fait en plusieurs étapes. Dans un premier temps a été créé le système informatisé d'échange d'informations sur les casiers judiciaires (ECRIS) afin de permettre l'échange des données relatives aux condamnations entre Etats membres. Ce système découle de la décision-cadre 2008/675 JAI du Conseil du 24 juillet 2008 qui impose la prise en compte des condamnations pénales antérieures, peu importe le pays membres dans lesquelles elles ont été prononcées lorsqu'une nouvelle procédure est engagée à l'encontre de la personne, renforçant ainsi la coopération entre Etats. Répondant à cet objectif, le système ECRIS est un traitement qui permet l'interconnexion des casiers entre eux. Aussi, sur demande, les données peuvent être échangées notamment pour accéder à certaines professions par exemple[1391]. Créé par la décision 2009/316 en date du 6 avril 2009[1392], il repose sur un « système informatique décentralisé »[1393], les données sont stockées sur des bases de données sécurisées gérées par les Etats membres et fonctionnant par cryptage des données[1394]. Il ne s'agit pas d'un droit d'accès

[1388] Ce dispositif est encadré s'agissant des questions intéressant la sécurité des données et leur finalité.
[1389] C'est-à-dire sans envisager nécessairement les effacements anticipés.
[1390] Voir sur la question de l'interconnexion, JJ. Lavenue, « L'interopérabilité et l'interconnexion des fichiers de police : enjeux et ambiguïté du rapport dialectique entre principe d'efficacité et protection des libertés », *op. cit.*, 2014.
[1391] Directive 2011/92/UE du 13 décembre 2011 relative à la lutte contre les abus sexuels et l'exploitation sexuelle des enfants, ainsi que la pédopornographie.
[1392] Directive 2009/316/JAI du 6 avril 2009 relative à la création du système européen d'information sur les casiers judicaires.
[1393] *Ibid*. cdt. 11.
[1394] *Ibid*. art. 3.

direct en ligne mais bien d'une interconnexion par laquelle les systèmes échangent des données relatives à un même individu[1395].

Le système a récemment été complété par le règlement 2019/816 du Parlement européen et du Conseil en date du 17 avril 2019 qui créé le système centralisé dénommé ECRIS-TCR[1396]. Dans un but annoncé de renforcer la sécurité sur tout le territoire de l'Union européenne, le système repose sur la prise en compte des données relatives aux condamnations sur tout le territoire y compris s'agissant des personnes ressortissantes de pays tiers[1397]. Ces deux traitements ont vocation à contenir des données d'identifications. Les données sont conservées au fichier central du moment qu'elles sont inscrites aux casiers judiciaires nationaux[1398]. L'effacement des données est, par principe, automatique[1399]. En tant que fichiers interconnectés, toute modification sur le casier entraine la même modification sur ECRIS-TCN[1400]. Si en termes de durées de conservation ces nouveaux dispositifs ne semblent pas soulever de questions particulières, se pose néanmoins la question de l'effectivité du droit à l'oubli. Par principe toute action en rectification ou effacement engagée sur le casier national entrainera la même conséquence sur le casier européen mais des interrogations subsistent quant aux accès à ces fichiers qui permettent que les données soient diffusées hors des frontières et constituent, de fait, une limitation à l'effectivité du droit à l'oubli. Cette question des limites territoriales du droit à l'oubli trouvent également à se poser s'agissant du droit au déréférencement[1401].

2° Les limites du droit à l'oubli conséquence du traitement massif des données judiciaires

503. L'oubli rendu difficile par le développement exponentiel du nombre de fichiers de police – La mise en pratique du droit à l'oubli se trouve nécessairement impactée par la multiplication du nombre de fichiers de police. Les différents rapports rendus en la matière font état d'un nombre croissant de fichiers au point qu'il parait difficile d'en établir la liste

[1395] Conformément aux dispositions de la décision-cadre 2009/315/JAI du Conseil du 26 février 2009 concernant l'organisation et le contenu des échanges d'informations extraites du casier judiciaire entre les Etats membres.
[1396] Règlement (UE) 2019/816 du Parlement européen et du Conseil du 17 avril 2019 portant création d'un système centralisé permettant d'identifier les États membres détenant des informations relatives aux condamnations concernant des ressortissants de pays tiers et des apatrides (ECRIS-TCN), qui vise à compléter le système européen d'information sur les casiers judiciaires, et modifiant le règlement (UE) 2018/1726 .
[1397] *Ibid*. cdt 1 à 3.
[1398] Règlement (UE) 2019/816 du Parlement européen et du Conseil du 17 avril 2019, Art. 8.
[1399] *Ibid*.
[1400] Règlement (UE) 2019/816 du Parlement européen et du Conseil du 17 avril 2019, Art. 9.
[1401] V. *infra* n°507.

exhaustive[1402]. En plus du développement du nombre de fichiers, on assiste à un élargissement des mentions fichées et des personnes visées par les traitements. Aussi, l'utilisation faite de ces données tant en termes d'accès que de finalités multiples soulève des interrogations sur l'effectivité d'un possible oubli. Si cela s'inscrit dans un désir toujours plus affirmé de prédire et anticiper[1403], ce fichage massif, peut constituer une atteinte aux libertés individuelles, et une entrave dans la mise en œuvre d'un droit à l'oubli.

504. L'oubli rendu difficile du fait de l'existence de failles dans le système – Il a souvent été fait référence aux erreurs contenues dans les fichiers de police et les fichiers judiciaires et leur absence de mise à jour. La Commission nationale de l'informatique et des libertés a, à plusieurs reprises, alerté sur ce phénomène et notamment dans un rapport de contrôle des fichiers de 2013[1404]. Ces erreurs peuvent conduire à ce que certaines données soient toujours conservées au sein des fichiers alors qu'elles auraient dû être « oubliées », ce qui en conséquence, porte une atteinte excessive aux droits et libertés si l'on se fonde sur les critères de licéité de finalité et exactitude des données.

Sur cette question, l'interconnexion a pu être présentée comme la solution pour une mise à jour effective des fichiers, comme par exemple en interconnectant le fichier d'antécédents au logiciel de la chaine pénale Cassiopée, ce qui témoigne une fois de plus des difficultés et enjeux de l'interconnexion de données, tantôt solution en faveur d'un droit à l'oubli effectif, tantôt frein à ce droit[1405].

Bien que non absolu le droit d'être oublié par les autorités judiciaires se trouve délimité par les textes, la question est néanmoins plus complexe s'agissant du potentiel droit d'être oublié par la collectivité.

§2. Le droit d'être oublié de la mémoire collective : un droit émergent mais limité

505. Oubli et mémoire collective – Le droit d'être oublié renvoie nécessairement à la volonté d'être oublié de tous. Il s'agit pour l'individu d'obtenir de la collectivité qu'elle ne l'associe

[1402] V. Gautron, La prolifération incontrôlée des fichiers de police, *AJ Pénal*, 2007 ; 57. Ce constat fait en 2007 est d'autant plus d'actualité aujourd'hui.
[1403]Voir sur le sujet, V. Gautron, Une mémoire policière hypertrophiée : la fin du droit à l'oubli ?, *Les cahiers de la justice*, 2016, 607.
[1404] Rapport CNIL du 13 juin 2013 adopté en assemblée plénière relatif au contrôle des fichiers d'antécédents du ministère de l'intérieur, *op. cit.*
[1405] V. *Supra* n°238.

plus dans le futur à son passé judiciaire. Si les fichiers judiciaires et le casier judiciaire national, notamment, s'effacent, la question demeure plus complexe s'agissant des données diffusées publiquement que ce soit par les écrits papiers et plus encore s'agissant des écrits numériques qui se trouvent diffusés, recopiés sans limitation ne laissant à l'individu concerné que peu de contrôle sur les données qui le concernent. Cette diffusion se trouve alors non pas justifiée par les besoins de la justice comme en matière de fichiers de police et judiciaires mais par le droit à l'information et la liberté de la presse. Dans une société qui prône le droit à l'information il faut s'interroger sur les problématiques liées à la rediffusion des données du procès en termes de droit à l'oubli (A.), ce qui amène à s'interroger sur l'effectivité d'un réel droit à l'oubli s'agissant de son passé judiciaire (B.).

A. Les problématiques liées à la rediffusion des données du procès

506. Problématique du contrôle des données diffusées sur internet – La première limite à laquelle se trouve confronté le droit à l'oubli est celle de la rediffusion des données sur internet. La question sous jacente est celle de la place de l'oubli face à la mémoire d'internet. Finalement si l'oubli semble encadré s'agissant des données traitées et conservées dans les fichiers de police ou judiciaires, quant est-il des données ayant fait l'objet d'une diffusion sur internet et par voie de presse ? L'oubli se trouve alors confronté à une mémoire diffuse dans le sens où les informations sont relayées, rediffusées, copiées, rendant leur traçage, leur effacement et donc leur oubli difficile. Cela amène au premier constat d'un droit au déréférencement limité (1°) et d'un second constat d'une anonymisation des données imparfaite (2°).

1° Un droit au déréférencement limité

507. Le déréférencement comme outil du droit à l'oubli – Issu du droit prétorien et notamment de l'arrêt *Google Spain* de la Cour de justice de l'Union européenne, il convient de s'interroger sur la portée du droit au déréférencement comme outil du droit à l'oubli. Dans une décision du tribunal de grande instance de Paris du 20 avril 1983, les juges avaient estimé que l'oubli s'impose à tous y compris aux journalistes. Le droit à l'oubli était alors invoqué pour faire obstacle à la rediffusion relative à une affaire judiciaire[1406]. Force est de constater

[1406] Voir, T. Hassier, Droits de la personnalité rediffusion et droit à l'oubli, *op. cit.*, 2829.

que suite à cela, l'oubli et notamment le droit à l'oubli face à la rediffusion des données a été oublié. L'idée a refait surface avec l'arrêt *Google Spain* qui consacre le droit au déréférencement et permet aux individus d'obtenir des moteurs de recherche que leurs données personnelles n'apparaissent plus dans la liste des résultats d'une recherche effectuée à partir de leur nom. Toutefois la limite en termes de droit à l'oubli est évidente.

508. Le déréférencement comme outil limité du droit à l'oubli – Le déréférencement n'entraine pas l'effacement des données dans la base de données, il rend néanmoins l'accès à ces données plus difficile. Saisie sur renvoi préjudiciel, la Cour justice de l'Union européenne a eu l'occasion d'apporter des précisions sur ce droit au déréférencement dans deux arrêts en date du 24 septembre 2019[1407].

Dans le premier arrêt, la Cour de justice est venue préciser l'étendue territoriale du droit au déréférencement, précisant que ce dernier doit être de portée européenne[1408]. Dans le second, la Cour de justice a du se prononcer sur l'application du régime relatif aux données sensibles aux moteurs de recherche tel que défini par la directive 95/46/CE du 24 octobre 1995. Bien qu'abrogée depuis, le raisonnement est transposable au régime actuel régit par le règlement général sur la protection des données. De cet arrêt complexe, dont la synthèse reste difficile, il ressort néanmoins certaines lignes directrices. Ainsi, rappelant que les moteurs de recherche réalisent des traitements de données au sens de la loi, la Cour de justice de l'Union européenne précise que les dispositions particulières qui encadrent strictement le traitement de données sensibles sont applicables aux moteurs de recherche. Pour autant, cela ne revient pas à interdire aux moteurs de recherche le référencement de pages contentant des données sensibles, toutefois, les demandes de déréférencement concernant ces pages doivent être étudiées au vu de ce critère et des exceptions permettant le traitement de ces données[1409]. Néanmoins, la Cour de justice précise que le droit au déréférencement n'en est pas moins, par principe, automatique. Face aux autres intérêts en présence, notamment le droit à l'information, l'exploitant d'un moteur de recherche doit apprécier si le référencement est « strictement nécessaire »[1410] ou non à la protection de la liberté d'information. De plus, la Cour de justice précise que s'agissant des données relatives à des procédures judiciaires ou à

[1407] CJUE, Gde. ch., 24 septembre 2019, Aff. C-507/17, Aff. C-136/17.
[1408] La CNIL préconise elle un droit au déréférencement mondial seul, selon elle, susceptible d'assurer une réelle protection des droits des personnes.
[1409] L'arrêt vise les dispositions de l'article 8 de la directive du 24 octobre 1995 qui pose comme exception à l'interdiction du traitement de données sensibles le cas dans lequel les données ont été rendues publiques par l'individu concerné où celui dans lequel le traitement est mis en œuvre à des fins de constatation, d'exercice ou défense d'un droit en justice.
[1410] CJUE, Gde. ch., 24 septembre 2019, Aff. C-136/17, cdt. 68.

des condamnations, le responsable doit procéder au déréférencement si les données ne sont pas actualisées[1411]. Cette décision favorable au droit à l'oubli sur internet rappelle néanmoins ses limites.

La Cour de justice semble de fait, créer une responsabilité des exploitants de moteurs de recherche s'agissant des données contenues dans les documents web auxquels ils donnent simplement accès[1412]. Cette responsabilité n'est en réalité pas une responsabilité quant aux données contenues dans les documents mais plus une obligation pour les exploitants de moteurs de recherche d'opérer une vérification quant à la nature des données accessibles au regard des normes européennes[1413].

509. Le droit au déréférencement au regard des autres droits en présence – Par la suite, le Conseil d'Etat est venu, à l'occasion de treize décisions, faire une application de ces arrêts et apporter des précisions quant à la marche à suivre pour apprécier les demandes de déréférencement[1414]. Offrant des cas d'espèce très différents, ces décisions ont permis de dégager des lignes directrices sur l'application du droit au déréférencement et apportent des précisions utiles quant au droit à l'oubli. Ainsi pour reprendre une analyse doctrinale[1415], il ressort de ces décisions que si par principe l'exploitant doit répondre positivement aux demandes de déréférencement, le droit au déréférencement n'est pas absolu et doit être apprécié au regard des autres intérêts en présence. Aussi, la nature sensible des données doit amener l'exploitant du moteur de recherche à porter un regard particulier sur la demande au vu de l'ingérence dans la vie privée qu'engendre la diffusion de telles données. Cela ne lui interdit pas de référencer des pages web contenant des données sensibles mais le maintien dans la liste ne peut être justifié que par l'intérêt public. S'agissant des liens menant à des données pénales, relatives à des condamnations notamment, le Conseil d'Etat semble prendre

---

[1411] *Ibid*. cdt. 71.

[1412] Voir, G. Desgens Pasanau, Droit au déréférencement : nouvelles décisions de la CJUE, de la Cour de cassation et du Conseil d'Etat, *Communication commerce électronique*, n°2 février 2020, étude 3. B. du Chaffaut, Demandes de déréférencement, droit à l'oubli, traitement de données aux fins de journalisme : état des lieux et perspective, *Legipresse*, 2020, p.79.

[1413] CJUE, Gde. ch., 24 septembre 2019, *op. cit*., cdt. 47.

[1414] CE, 6 déc. 2019, n° 391000, M. A. c/ CNIL, JurisData n° 2019-021942, CE, 6 déc. 2019, n° 393769, M. A. c/ CNIL, JurisData n° 2019-021946, CE, 6 déc. 2019, n° 395335, X. c/ CNIL, JurisData n° 2019-021954, CE, 6 déc. 2019, n° 397755, M. A. c/ CNIL, JurisData n° 2019-023333, CE, 6 déc. 2019, n° 399999, M. A. c/ CNIL, JurisData n° 2019-022603, CE, 6 déc. 2019, n° 401258, M. A. c/ CNIL, JurisData n° 2019-021955, CE, 6 déc. 2019, n° 403868, M. A. c/ CNIL, JurisData n° 2019-021947, CE, 6 déc. 2019, n° 405464, M. A. c/ CNIL, JurisData n° 2019-021770, CE, 6 déc. 2019, n° 405910, M. A. c/ CNIL, JurisData n° 2019-021767, CE, 6 déc. 2019, n° 407776, A. c/ CNIL, CE, 6 déc. 2019, n° 409212, M. A. c/ CNIL, JurisData n° 2019-021949, CE, 6 déc. 2019, n° 429154, X c/ CNIL, JurisData n° 2019-021755 , CE, 6 déc. 2019, n° 423326, M. A. c/ CNIL.

[1415] La présentation ci après reprend l'analyse de N. Mettalinos, Clarification du Conseil d'Etat sur l'application du droit au déréférencement sur internet, *Communication commerce électronique*, n°2, février 2020, comm.17.

en compte le critère temporel considérant que lorsqu'il est fait état d'une affaire ancienne la demande de déréférencement doit être accordée. Si la Cour de justice a affirmé la nécessité d'observer le caractère actuel des données mises à disposition, le Conseil d'Etat affirme ici que le statut public de la personne visée permet de rejeter une demande de déréférencement alors même que les données ne sont plus d'actualité. La doctrine soulève très justement les problématiques qui restent sans réponse, comme savoir quels sont les moteurs de recherche visés par ces dispositions[1416]. Aussi, il n'est fait référence qu'aux recherches effectuées à partir du nom ce qui semble exclure les cas dans lesquels les données sont accessibles par un autre mode de recherche[1417] soulevant ici la question la pseudonymisation et de l'identification indirecte des individus. En cela le droit au déréférencement a un champ d'application plus restreint visant l'effacement des données accessibles par le nom, alors que le règlement général sur la protection des données et la loi informatique et libertés visent les données permettant l'identification directe et indirecte.

2° Une anonymisation des données insuffisante à assurer l'effectivité d'un droit à l'oubli

510. La limite au droit à l'oubli de par l'anonymisation imparfaite des décisions de justice – Le droit à l'oubli est aussi limité du fait du caractère imparfait de l'anonymisation des données diffusées. Revenant ici sur la question de la diffusion des décisions de justice et par leur mise en *open data*[1418], la problématique déjà soulevée du fait de la possibilité d'identifier les personnes lorsque la donnée est simplement pseudonymisée, constitue une limite au droit à l'oubli. Dans sa délibération du 29 novembre 2001, la CNIL préconisait que les éditeurs de bases de données judiciaires ne mentionnent ni le nom ni l'adresse des individus visés par égard à « l'indispensable droit à l'oubli »[1419]. Comme vu précédemment[1420], dans la pratique les données des jugements sont en réalité pseudonymisées ce qui rend l'identification des individus possible par le recoupement de données. De fait, bien que bénéficiant de ce système protecteur, on peut envisager que des données publiées sur internet permettent de faire le rapprochement avec l'individu concerné et entrave le possible

[1416] *Ibid*. L'auteure fait notamment référence aux moteurs de recherche qui sont inclus dans des sites internet.
[1417] *Ibid*.
[1418] V. *supra* n°412 s.
[1419] Bilan de l'application de la recommandation de la CNIL du 29 novembre 2001 sur la diffusion de données personnelles sur Internet par les banques de données de jurisprudence : pour un encadrement législatif renforçant la protection des données à caractère personnel en matière de diffusion de décisions de justice. Adopté par la commission le 19 janvier 2006.
[1420] V. *supra* n°418 s.

« droit à l'oubli » du fait des risques réels de réidentification. Néanmoins, les dispositions prévues dans la loi du 23 mars 2019 et le décret du 29 juin 2020 semblent plus protectrices en permettant, le cas échéant, de demander à ce que des données supplémentaires soient occultées avant diffusion du jugement[1421].

511. L'application des dispositions aux organes de presse – La notion de droit à l'oubli renvoie nécessairement à des interrogations liées à la diffusion de données par les organes de presse. En relatant des données relatives aux procès, par exemple, et notamment de manière numérique se pose la question de l'effectivité du droit à l'oubli. La presse dispose d'un régime particulier issu de la loi de 1881 leur permettant notamment de faire des comptes-rendus fidèles des débats judiciaires[1422]. Il s'agit toutefois de s'interroger sur la mise en œuvre d'un droit à l'oubli s'agissant des données révélées par ce biais. Par exemple s'agissant des normes encadrant le traitement des données caractère personnel, l'article 17 du règlement général sur la protection des données pose comme exception au droit à l'effacement, le cas des données traitées dans le cadre de l'exercice de la liberté d'expression et du droit à l'information[1423]. Aussi, la loi informatique et libertés, dans une section qui y est consacrée, précise que les données traitées à des fins journalistiques, notamment, répondent à un régime dérogatoire permettant une conciliation entre protection des données à caractère personnel et liberté d'expression et d'information, visant toutefois le respect de normes déontologiques[1424]. Il apparait néanmoins envisageable de faire jouer le droit d'opposition au traitement de données pour motif légitime. Là encore, un tel litige amène les juges à mettre en balance des intérêts antagonistes. Aussi, si la demande est accueillie favorablement il n'en reste pas moins qu'une telle action peut conduire à anonymiser le document litigieux avec les failles que cela comprend[1425]. La Cour de cassation s'est justement prononcée sur le sujet. Dans un arrêt du 12 mai 2016, elle a considéré que « le fait d'imposer à un organe de presse, soit de supprimer du site internet dédié à l'archivage de ses articles, qui ne peut être assimilé à l'édition d'une base de données de décisions de justice, l'information elle-même contenue dans l'un de ces articles, le retrait des nom et prénom des personnes visées par la décision privant celui-ci de

[1421] V. *supra* n°
[1422] Art. 41 de la loi du 29 juillet 1881 sur la liberté de la presse.
[1423] Art. 17 3^{e} a) du règlement général sur la protection des données du 2 avril 2016.
[1424] Art. 80, 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.
[1425] Pour rappel, l'anonymisation au sens stricte semble impossible puisqu'elle sous entend de retirer tous les éléments permettant une identification des individus même par recoupement de données. La réalité renvoie davantage à une pseudonymisation qui de fait permet d'identifier les personnes.

tout intérêt, soit d'en restreindre l'accès en modifiant le référencement habituel, excède les restrictions qui peuvent être apportées à la liberté de la presse »[1426]. Dans cet arrêt, la Cour de cassation rappelle donc que la diffusion numérique de la presse n'est pas assimilable à des bases de données jurisprudentielles et que le fait de retirer les éléments d'identification des individus visés va à l'encontre de sa mission d'information. Aussi, la Cour de cassation précise que le fait d'agir sur le référencement des données en question va de la même manière à l'encontre de la liberté de la presse.

Dans sa délibération du 29 novembre 2001, la CNIL appelait les organes de presse à une réflexion déontologique sur la question d'un droit à l'oubli qui semble difficile à atteindre face à « l'hypermnésie numérique »[1427]. En cela, le droit au déréférencement semble constituer le seul mode d'action effectif avec toutefois ses limites. Ces raisonnements poussent à s'interroger de manière plus générale sur l'effectivité d'un droit à l'oubli s'agissant des données traitées au cours de procédures judiciaires.

B. L'effectivité d'un réel droit à l'oubli s'agissant de son passé judiciaire

512. L'oubli, notion ou concept juridique – Les raisonnements précédents appellent nécessairement à s'interroger sur l'existence réelle d'un droit à l'oubli en tant que droit subjectif. Sans prétendre ici apporter ici une réponse aboutie sur la question, quelques éléments peuvent néanmoins être avancés pour étayer cette réflexion. En reprenant la notion de droit à l'oubli telle qu'elle a été développée par la doctrine notamment et en observant la consécration qui en a été faite par les textes on comprend l'évolution même du concept d'oubli. Il convient donc, à partir de l'émergence des notions relatives à l'oubli (1°), d'observer sa conceptualisation par les textes (2°).

1° L'émergence de notions relatives à l'oubli

513. Des notions d'oubli – Née dans la doctrine puis affirmée dans la jurisprudence, la notion d'oubli a pu être présentée comme un droit pour les individus à ne plus être associés à leur

[1426] Cass., civ. 1ère, 12 mai 2016, *pourvoi* n°15-17729. P. Sergeant, Pratique contentieuse. Le droit à l'oubli inopposable aux éditeurs de presse : l'arrêt de la Cour de cassation du 12 mai 2016, *Communication commerce électronique*, n°9, septembre 2016, 14. N. Metallinos, Droit d'opposition et liberté de la presse, *Communication commerce électronique*, n°7-8, juillet 2016, comm.64.

[1427] N. Metallinos, Droit d'opposition et liberté de la presse, *op. cit.*

passé judiciaire. Ce droit repose alors sur un critère temporel comme renvoyant à l'idée de pardon accordé passé un certain délai ou à celle de « prescription ».

Dans la jurisprudence, l'oubli est ensuite invoqué sur le fondement du droit au respect de la vie privée, la révélation des données dans le temps causant alors un préjudice à l'individu en droit d'obtenir l'oubli.

Il faut admettre que la notion d'oubli a toujours été présente en droit notamment s'agissant des dispositions encadrant la prescription, des normes encadrant les durées de conservation des données ou les procédures de réhabilitation ou d'amnistie.

La première étape dans une esquisse de consécration réside dans la reconnaissance d'un droit au déréférencement sur internet qui témoigne de l'orientation donnée à l'oubli conséquence des évolutions technologiques. La seconde étape, découlant de la réforme européenne sur la protection des données, réside dans la consécration du droit à l'effacement des données pour motifs légitimes à l'article 17 du règlement général, peut-être, maladroitement désigné comme « droit à l'oubli ». Mais finalement on peut s'interroger sur l'existence d'un réel droit subjectif à l'oubli.

2° La conceptualisation de l'oubli

514. Oubli, effacement, déréférencement – Le droit à l'oubli suppose un droit pour l'individu d'exiger de la société qu'elle oublie les données qui le concerne et lui offrir les moyens d'obtenir cet oubli. Comme cela a pu être dit très justement, « le droit ne peut pas garantir l'oubli »[1428]. *A contrario*, si l'on fait le parallèle avec le droit à l'information, il apparait plus évident de pouvoir disposer de prérogatives visant à obtenir ladite information. Plus clairement, on peut exiger d'obtenir une information que l'on ne détient pas et à laquelle on est en droit d'avoir d'accès, mais beaucoup moins qu'une information soit oubliée. Le législateur européen et le législateur interne sous son influence certaine ont consacré un droit à l'effacement des données sous conditions. Ce droit à l'effacement et de manière générale les droits consacrés en termes de traitement de données témoignent davantage de la reconnaissance d'un droit à « l'autodétermination informationnelle » que d'un « droit à » l'oubli[1429]. Les moyens dont disposent les individus concernés par un traitement couplés aux normes encadrant la gestion des données personnelles judiciaires sont des outils de l'oubli.

[1428] D. Dachenaud, *Le droit à l'oubli*, Centre de recherche juridique, travaux déposés en février 2014, *in*, [http://www.gip-recherche-justice.fr/publication/view/le-droit-a-loubli/].
[1429] D. Dachenaud, *Le droit à l'oubli numérique*, Larcier, 2015.

Toutefois, la consécration par le législateur semble enfermer cette notion dans des dispositions visant l'effacement des données numériques et le déréférencement sur les moteurs de recherche ce qui est plus restreint que la notion d'oubli telle qu'elle a pu être définie par le passé.

515. Limites à l'oubli – Les droits permettant la mise en œuvre de l'oubli connaissent de nombreuses limites. Dès lors, ils se trouvent dans un premier temps limités par les besoins de la justice qui suppose que soient conservées des données à caractère personnel dans le cadre d'enquêtes, ou s'agissant des condamnations et d'autre part, par la mise en concurrence avec d'autres droits et libertés. En cela, il parait plus opportun de parler d'un droit à l'effacement pour motifs légitimes. Un droit à l'oubli numérique semble néanmoins consacré s'agissant des données relatives aux mineurs avec un réel droit à obtenir l'effacement des données.
Finalement face au nombre croissant de fichiers contenant des données à caractère personnel, à l'augmentation des droits d'accès à ces données, à des durées de conservation qui s'allongent[1430] d'un côté et au développement des bases de données en open data de l'autre, le droit à l'oubli semble dans ce domaine relever davantage d'un objectif à atteindre que d'un « droit à ».
Il s'agit donc davantage d'un droit à « l'autodétermination informationnelle » qui met à la disposition des individus des moyens leur permettant de requérir auprès du responsable du traitement l'effacement de leurs données, sans pour autant leur garantir qu'ils soient « oubliés ».

Conclusion du titre 2

516. La réorganisation de la diffusion des décisions – Les récents textes ont réorganisé la publicité de la justice avec d'un côté le droit d'accès aux décisions et de l'autre la mise en *open data* de celles-ci, consacrant ainsi la publicité numérique des décisions de justice. Cela soulève des interrogations en termes de droits des individus et protection de leurs données. La loi de programmation de 2019 et le décret du 29 juin 2020 ont précisé les règles relatives à l'occultation des données identifiantes, prévoyant différents régimes. S'agissant de la mise en *open data*, ils prévoient une occultation de principe des noms et prénoms et la possibilité de demander des occultations supplémentaires. En matière de droit d'accès, les données

[1430] V. Gautron, Une mémoire policière hypertrophiée : la fin du droit à l'oubli ?, *Les cahiers de la justic*e, *op. cit.*

identifiantes sont occultées lorsque la divulgation est de nature à porter atteinte à la vie privée des parties ou des tiers, soulevant de fait la question de l'appréciation de cette potentielle atteinte. De plus, la remise de copies au tiers soulève évidemment des interrogations sur les risques attachés à une diffusion massive des décisions et les potentielles rediffusions successives rendant les données difficilement traçables. Ces textes s'inscrivent dans le mouvement actuel de diffusion et de transparence mais certaines craintes légitimes demeurent malgré les garanties posées.

517. Une gestion encadrée des données fichées – Les données faisant l'objet d'une collecte et d'un fichage au cours d'une procédure répondent au critère de nécessité et de finalité. Par principe, les données ne peuvent être conservées que le temps nécessaire et doivent être effacées passé ce délai. En matière de données judiciaires, les textes encadrant les fichiers prévoient les modalités de gestion avec un principe de mise à jour d'office de celles-ci. Les individus concernés disposent d'un droit d'accès et de rectification sur ces données et pour certains fichiers peuvent demander l'effacement anticipé des données. Ces droits réaffirmés et renforcés par le règlement général sur la protection des données et la loi informatique et liberté dans sa nouvelle rédaction témoignent de la volonté de donner à l'individu une information claire concernant ses données traitées et un certain pouvoir d'action sur celles-ci. On comprend aisément les avancées rendues possibles par le fichage notamment en matière d'identification, les risques étant en la matière attachés à l'étendue du fichage et notamment au fichage massif qui peut alors soulever la question de l'atteinte aux libertés fondamentales et au-delà celle de l'utilité d'un tel fichage.

518. Des droits affirmés et renforcés pour les individus – Face aux enjeux et risques liés au développement des nouveaux moyens de communication, il a fallu repenser les normes qui encadrent le traitement de données à caractère personnel. Cela est passé notamment par la réaffirmation de droits pour les individus. De manière générale ont été réaffirmés les droits d'accès, de rectification, d'opposition et d'effacement des données. Une des questions qui se posent est celle des données judiciaires qui sont diffusées sur internet notamment par la presse et font l'objet de rediffusion. Le droit à l'effacement numérique ou droit au déréférencement a été consacré comme l'adaptation des droits préexistants au monde du numérique. S'agissant des données de justice, ces droits peuvent prendre la forme de demandes d'occultation de données présentées avant leur diffusion.

519. Des droits néanmoins limités et un droit à l'oubli discutable – Malgré l'affirmation de droits s'agissant de la diffusion de données, ces derniers trouvent des limites tant quant à leur portée que leur effectivité. En effet, certains traitements n'ouvrent pas droit à une action quelconque. De plus, l'exercice des droits peut être complexifié par la diffusion massive et éparse de données sur internet. Enfin une autre limite tient à l'effectivité de la protection assurée par les procédés de pseudonymisation qui permettent parfois l'identification indirecte des individus. L'oubli apparait donc comme limité s'agissant de la mémoire judiciaire et semble illusoire s'agissant de la mémoire collective. Moins qu'un droit à l'oubli au sens strict du terme, le législateur a davantage consacré un droit à « l'autodétermination informationnelle ».

Conclusion de la partie 2

520. Une diffusion élargie au nom du principe de transparence et du droit à l'information – Le constat qui peut être fait est celui d'une justice qui se veut de plus en en plus accessible et de plus en plus transparente. Cela passe, par exemple, par une communication accrue des données d'enquête et d'instruction. Cette question soulève des désaccords quant au bien fondé du secret dans cette phase de l'instruction. Néanmoins, le droit à l'information peut-il se faire au détriment du bon déroulement de l'enquête ? Il apparait essentiel et délicat de trouver le juste équilibre entre ces intérêts parfois antagonistes.

521. Les risques d'une diffusion massive des décisions face au droit à l'oubli – La mise à disposition des décisions soulève aussi des interrogations quant aux conséquences d'une mise à disposition massive des décisions, malgré les mesures d'occultation. Il est acquis que les procédés d'occultation ou de pseudonymisation n'empêche pas une identification des individus par recoupement de données.

Cela pose la question plus générale de la concrétisation d'un droit à l'oubli face à une médiatisation grandissante des affaires et une diffusion massive des décisions. Ce droit à l'oubli apparait en l'état très illusoire.

Le phénomène de dématérialisation des procédures soulève de la même manière des interrogations quant au traitement de données de procédure qui seraient exclusivement numériques et stockées informatiquement au nom d'une plus grande célérité des procédures notamment. Cela s'inscrit dans les évolutions générales que connait la société moderne mais n'est pas sans soulever des interrogations notamment en termes de traitement et protection des données personnelles.

CONCLUSION GENERALE

522. Une protection des données évolutive – On ne peut nier l'engouement récent sur la question du traitement des données personnelles qui est attaché, sans aucun doute, à l'adoption du règlement général sur la protection des données en 2016 et sa transposition en droit interne en 2018. Toutefois, la protection des données n'est pas nouvelle, il est utile de rappeler que des normes existaient avant l'adoption du « paquet européen ».
Il est évident que la loi informatique et libertés et la directive du 24 octobre 1995 nécessitaient d'être repensées et adaptées aux évolutions de la société.
A plus ou moins bon escient, le traitement de données et notamment de données à caractère personnel a connu une progression exponentielle. Les nouveaux moyens technologiques et de communication permettent une captation et une diffusion massive des données de manière rapide et sans limites de frontières.

523. Le traitement nécessaire de données en matière judiciaire – C'est une évidence, toute procédure repose sur un traitement de données. En matière de traitements de données judiciaires, il est certain que toutes les évolutions technologiques et scientifiques ont permis des avancées bénéfiques. La collecte et le fichage de données permet de faciliter la résolution des affaires notamment par l'identification des auteurs d'infractions ainsi que de développer la coopération internationale. La transmission numérique des données de procédure permet une meilleure célérité de celle-ci. Enfin, la diffusion des décisions en *open data* permet une meilleure information des justiciables. Néanmoins il convient d'observer avec prudence les dérives que pourrait engendrer un traitement massif de données ainsi que leur dématérialisation et mise en *open data*.

524. Les risques liés à un fichage massif de données – S'agissant plus particulièrement du fichage de données à caractère personnel, le risque réside dans un premier temps dans l'ampleur des données visées et des individus concernés.
La CNIL a souvent alerté sur les risques d'un traitement massif de données. Les décrets récents relatifs aux fichiers PASP et GIPASP et qui permettent une extension des données fichées, comme par exemple des données relatives aux opinions politiques ou aux activités sur

les réseaux sociaux, soulèvent des interrogations quant au fichage massif de données sensibles[1431].

Aussi, bien qu'il ne s'agisse pas à proprement parler d'un fichier judiciaire, il convient de citer le fichier des titres électroniques sécurisés (TES)[1432] qui centralise des données biométriques liées à l'identité, le visage et les empreintes digitales des individus possédant une carte d'identité ou un passeport. Les données sont accessibles par les autorités administratives et judiciaires en matière de prévention et de répression des atteintes aux intérêts fondamentaux de la Nation. La CNIL a rendu un avis alarmant sur les risques d'un fichage d'une telle ampleur, notamment en cas de piratage du système, d'autant plus que le fichier contient des données sensibles[1433]. De plus, aucune analyse d'impact n'avait été faire malgré le caractère sensible des données visées. Ce fichier n'est pas sans rappeler le « fichier des honnêtes gens » censuré quelques années plus tôt par le Conseil constitutionnel du fait notamment de l'ampleur des personnes visées et de la nature des données concernées[1434].

Bien que la finalité du fichier puisse être légitime, l'ampleur du fichage doit être observée avec prudence au regard de tous les risques potentiels encourus. Ces risques peuvent être d'ordre matériel avec notamment la menace d'éventuelles intrusions dans les systèmes bien que ceux-ci soient très sécurisés. Il faut aussi être prudent quant aux potentielles utilisations futures des données notamment en termes de rapprochement ou d'interconnexions. Enfin, le fichage massif qui viserait à conserver des données relatives à l'entière population soulève évidemment des interrogations en termes de libertés fondamentales et dans une moindre mesure d'efficience d'un tel traitement.

525. Les risques liés à une diffusion massive des données – Au-delà de l'extension des données fichées et traitées dans le cadre de procédures, les risques résident dans la diffusion de plus en plus importante des données procédurales. Le risque réel est ici attaché à la diffusion massive des données sur internet. De manière générale les données diffusées sur

[1431] V. *supra* n°157.

[1432] Décret n° 2016-1460 du 28 octobre 2016, autorisant la création d'un traitement de données à caractère personnel relatif aux passeports et aux cartes nationales d'identité. M. Quéméner, Présentation du décret du 28 octobre 2016 autorisant la création d'un traitement de données à caractère personnel relatif aux passeports et aux cartes nationales d'identité (TES), Dalloz IP/IT, 2017, 58.

[1433] Délibération CNIL n° 2016-292 du 29 septembre 2016 portant avis sur un projet de décret autorisant la création d'un traitement de données à caractère personnel relatif aux passeports et aux cartes nationales d'identité.

[1434] Cons. const. 2012-652 DC du 22 mars 2012. D. Poupeau, Le fichier des « honnêtes gens » fait des vagues, *AJDA*, 2016, 2137. Sur la Loi n° 2012-410 du 27 mars 2012 relative à la protection de l'identité. Le fichier créé a souvent été qualifié de « fichier des gens honnêtes », ou « fichier des honnêtes gens ».

internet font l'objet de rediffusions qui rendent illusoires l'exercice des droits des individus concernés et du droit à l'effacement notamment.

A ce sujet, la mise en *open data* des décisions de justice interroge. Si une protection semble assurée par l'occultation de certaines données identifiantes, avec la possibilité de demander une protection supplémentaire, l'effectivité des procédés de pseudonymisation a toujours montré ses limites[1435]. Le recoupement de données rend parfois possible l'identification des individus concernés.

526. Le nécessaire renforcement des contrôles opérés sur certains traitements – Les contrôles opérés sur les traitements de données sont réels, encore faut-il qu'ils soient effectifs. La CNIL s'est vu retirer son pouvoir d'autorisation *a priori* sur les traitements de données au profit d'une plus grande responsabilisation des acteurs et un renforcement de ses pouvoirs *a posteriori*. En matière de fichiers judiciaires si elle rend par principe des avis sur les traitements susceptibles de porter atteinte aux droits et libertés, il faut mentionner que ces avis ne sont pas contraignants. Force est de constater que dans la pratique la commission n'est pas toujours saisie d'une demande d'avis et que lorsque cela est le cas, un avis défavorable n'est pas toujours suivi d'effets[1436]. Le contrôle *a posteriori* s'il est effectif dans les textes avec une augmentation des pourvoirs de sanction attribués à la CNIL, reste résiduel en pratique[1437]. La CNIL fait face à un nombre croissant de plaintes, liées sans aucun doute à l'engouement provoqué par l'adoption du règlement général, qui se traduit dans la pratique par des délais de traitement longs[1438]. De plus, il apparait que des sanctions semblent assez rarement prononcées, bien que l'année 2020 ait été marquée par le prononcé d'une sanction record à l'encontre d'une GAFA pour non respect du droit d'opposition notamment.

S'agissant du contrôle de constitutionnalité le constat est celui d'une censure rare sur la création des fichiers et aussi celui d'un recours tout aussi rare au mécanisme de la question prioritaire de constitutionnalité.

S'agissant du contrôle de conventionalité, il est admis que la Cour européenne des droits de l'homme opère davantage un contrôle de proportionnalité dans la mise en œuvre du fichier que sur sa création.

[1435] V. *supra* n°427

[1436] V. Gautron, *Fichiers de police*, Répertoire de droit pénal et de procédure pénale, 33-42.

[1437] *Ibid*.

[1438] Sur l'année 2019, la CNIL a reçu 14137 plaintes contre 11077 en 2018 soit une hausse de 27%. (Chiffres issus du bilan d'activité de la CNIL pour 2019). Il faut également mentionner les conséquences du contexte sanitaire de l'année 2020 en termes de traitement de données. La crise de la « COVID-19 » a entrainé une progression importante du recours aux traitements numériques de données.

Enfin, si le contrôle de légalité est plus effectif, le Conseil d'Etat ne prononce que très rarement l'annulation d'un acte qui porte création d'un fichier.
Face à la multiplication des traitements de données judiciaires, il semble opportun de garantir la mise en œuvre de contrôles plus effectifs et de doter la CNIL des moyens nécessaires à ses nouvelles missions.

527. La protection relative assurée par le secret – Entendue largement, la notion de secret renvoie tant aux données relevant du secret de l'enquête et de l'instruction, aux secrets professionnels et par extension aux données confidentielles ou pseudonymisées.
Dans tous les cas, le secret apparait comme étant relatif. Il est à confronter à d'autres droits et principes tels que le droit à la preuve, le droit à l'information ou le principe de publicité.
Si le droit à la preuve justifie de pouvoir obtenir ou présenter une donnée nécessaire dans le cadre d'une procédure[1439], l'équilibre semble plus délicat s'agissant de la diffusion de données protégées au nom du droit à l'information. La diffusion des données judiciaires par la publication soulève la question de l'effectivité de la protection assurée par l'occultation des données identifiantes et aussi celle de l'opportunité de retirer toutes ces données au risque que la décision ne soit plus compréhensible.
Il semble alors évident que la diffusion de données secrètes ne doit pas nuire au bon déroulement de l'enquête ou de l'instruction et qu'il faut ménager à la fois la procédure et le droit à l'information des justiciables. La diffusion massive des jugements en ligne soulève quant à elle la question de la possible existence d'un droit à l'oubli, qui semble en réalité assez illusoire.

528. L'équilibre délicat entre exploitation et protection – Le traitement des données repose sur une base légale et doit observer les principes de nécessité et de finalité. De plus, les textes ont d'un côté accentué la responsabilité des acteurs de traitements et réaffirmé l'existence de droit pour les individus concernés. Tout cela, doit permettre de mettre en balance les intérêts en présence et de trouver le juste équilibre.
Finalement, tout cela repose sur la recherche et l'obtention d'un équilibre entre le traitement nécessaire et la garantie pour les droits des individus. Cet équilibre semble toutefois délicat et précaire.

[1439] A. Bergeaud, *Le droit à la preuve*, pref. JC. Saint Pau, LGDJ, 2010.

Bibliographie

I. Manuels, traités, ouvrages

Ambroise Castérot C., Droits de la défense et secret de l'instruction, *in*, Guinchard, *Justice et droit du procès*, Dalloz, 2010.

Ach N. « Fichiers, sécurité, libertés : quelle conciliation ? », *in* B. Plessix, N. Deffains (dir.), *Fichiers informatiques et sécurité publique*, Presse universitaire de Lorraine, « Droit, politique, société », 2013, p. 15-35.

Bénéjat M., *Que reste-t-il du secret professionnel du notaire ?*, *in*, La responsabilité de l'avocat et du notaire, Travaux de l'Institut de sciences criminelles et de la justice, n°3, Cujas, 2013.

Benraïs L., Butruille-Cardew C., Fricero N., Gorchs-Gelzer B., Payan G., *Le guide des modes amiable de resolution des différends*, Dalloz, 3e ed., 2017/2018.

Bergaud A., *Le droit à la preuve*, préf. J.C. Saint-Pau, LGDJ, 2010, 588 p.

Bourgeois M., *Droit de la donnée. Principes théoriques et approche pratique*, LexisNexis, 2019

Boursier ME., *Le principe de loyauté en droit processuel*, LGDJ, 2003, 527 p.

Bouzat P., *La loyauté dans la recherche des preuves*, *in* Mélanges L. Hugueney. Problèmes contemporains de procédure pénale, Sirey, 1964, p. 172.

Cabrillac R., *Dictionnaire de vocabulaire juridique*, LexisNexis, 12e ed., 2021.

Cadiet L., Jeuland E., *Droit judiciaire privé*, LGDJ, 11e ed., 2020.

Capdepon Y., *Essai d'une théorie générale des droits de la défense*, préf. J.C. Saint Pau, Dalloz, 2013.

Carbonnier J., *Droit civil : Les personnes*, t. I, 20e éd., 1996, no 86.

Carbonnier J., *Droit civil, Introduction*, 27e ed. Thémis, PUF, 2002.

Chapus R., *Droit administratif général*, Montchrestien, 15e ed., 2001, p. 737.

Chambon M.., *Les fichiers, nouvel instrument de police administrative ?*, in Fichiers informatiques et sécurité publique, sous la direction de B. Plessix et N. Deffains, coll. Droit, Politique, Société, éd. Presse Universitaires de Lorraine, 2013, p. 91-108.

Cornu G., *Vocabulaire juridique*, PUF, 13e ed., 2020.

Dachenaud D*., Le droit à l'oubli numérique*, Larcier, 2015.

Décima O., *La juridictionnalisation de l'enquête pénale*, coll. Actes et Etudes, Cujas, 2015

Demarchi JR., *Les preuves scientifiques dans le procès pénal*, pref. C. Ambroise-Castérot, LGDJ, 2012, 414 p.

Decocq A., J. Montreuil, J. Buisson, *Le droit de la police*, Litec, 1998, p. 731

Doutremepuich C., *Les fichiers des empreintes génétiques en pratique judiciaire*, ed. Documentation française, 9 janvier 2007.

Elek C., *Le casier judiciaire*, Que sais-je ? n°2419, PUF, 1988

Farcy F., Gayraud JF., *Le renseignement criminel*, CNRS éditions, Biblis, 2011

Féral-Schuhl C., dans son ouvrage. *Cyberdoit*, Le droit à l'épreuve de l'internet, Dalloz, 8e ed., 2020/2021.

Fricero N., Guichard S., *Droit et pratique et de la procédure civile*, Dalloz, 2017-2018, 212.31.

Garapon A., Lassègue J., Justice digitale, PUF, 2018.

Gogorza A., L'autorisation judiciaire pendant la phase policière, *RSC* 2017, 247

Gouttenoire A., Le principe du contradictoire devant la Cour européenne des droits de l'homme, in *Le contradictoire dans le procès pénal – nouvelles perspectives*, Cujas, 2012, p. 65.

Guéry C., Chambon P., *Droit et pratique de l'instruction préparatoire*, Dalloz, 2018-2019, chapitre 562.

Guinchard S., Buisson J., Procédure pénale, LexisNexis, 12e ed., 2019

Guinchard S., Buisson J., *Procédure pénale*, LexisNexis, 11e ed., 2018, p. 366 et s.

Guinchard S., *Droit processuel : droits fondamentaux du procès*, 10 ed, Dalloz, 2019, p.1122.

Guinchard S., Ferrand F., Chainais C., Mayer L., Procédure civile, Dalloz, 6ème ed., 2019.

Guinchard S., Chanais C., Delicostopoulos C.S., Delicostopoulos L.S., Douchy-Oudot M, Ferrand F., . Lagarde X., Magnier V., Ruiz Fabri H., Sinopoli L., Sorel JM., *Droit processuel. Droits fondamentaux du procès*, 10 ed, Précis, Dalloz, Paris, 2019, p.1326 ets

Guicherd S., Caron-Fasan ML., Lesca N., Droit à l'oubli numérique : quel alignement entre chartes et pratiques ?, in Dechenaud David, *Le droit à l'oubli numérique, données nominatives, approches comparée*, Larcier, 2014.

Kayser P., "Le principe de la publicité de la justice dans la procédure civile", *in* mélange Hébraud, *Dalloz*, 1981, p. 515.

Labbée X., La fin du monde, la fin du droit ou la transition juridique ?, *Dalloz* 2019, p. 78

Lardeux G., *Du droit de la preuve au droit à la preuve,* Dalloz, 2012, p.1596.

Malabat V., *Droit pénal spécial*, Paris, Dalloz, Hypercours : cours et travaux dirigés, 7e éd., 2015, p. 248, n°461.

Massis T., « La transparence et le secret, champ sociale débats de conscience », *in Etudes*, 2001/6, Tome 396, p.751-761.

Matsopoulou H., L'illégalité des surveillances par « géolocalisation » autorisées par le ministère public, *Dalloz*, 2014, p. 115.

Orwell G., *1984*, Gallimard, 1950.

Pradel J., *Procédure pénal*, Cujas, 2013, 17e ed., 848, p. 773.

de Terwangne C., « Droit à l'oubli, droit à l'effacement ou droit au déréférencement ? Quand le législateur et le juge européens dessinent les contours du droit à l'oubli numérique », *in Enjeux européens et mondiaux de la protection des données personnelles* (sous la dir. de A. GROSJEAN), Bruxelles, Larcier, 2016.

Tolkien J.R.R., Le seigneur des anneaux, parus en 1954

Truilhé-Marengo E., Preuve scientifique, preuve juridique, Larcier, 2011.

Van Compernolle J., *Quelques réflexions sur un principe émergent : la loyauté procédurale*, *in* Mélanges Guinchard, Dalloz, 2010, p. 413.

Vergès E., Vial G., Leclerc O., *Droit de la preuve,* PUF, 2015.

II. Thèses, mémoires

Copain C, *L'encadrement de la contrainte probatoire en procédure pénale française*, Joly-Sibuet E (dir.), thèse de doctorat, droit, université de Lyon 3, 2011, 633 p.

H. Lavedrine, *L'expertise judiciaire,* Y. Mayaud (dir.), Master de droit pénal et sciences pénales, Université Panthéon-Assas Paris II, 2014.

A.M. Leroyer, *Les fictions juridiques,* Thèse, sous la direction de M. Gobert, Paris 2, 1995.
A. Ouattara, *L'accès à la justice à l'épreuve du numérique*, dir. C. Tirvaudey, Mémoire, Droit, CRJFC, 30 septembre 2020, 102 p.

C. Quennesson, *Mineur et secret*, A. Gouttenoire (dir.), thèse de doctorat, droit privé et sciences criminel, Université de Bordeaux, 2017, p. 282

C. Ribeyre, *La communication du dossier pénal*, pref. P. Maistre du Chabon, LGDJ, 2007, 708 p.

B. Roussel, *Les investigations numériques en procédure pénale*, Thèse, Bordeaux, 2020

J.C. Saint-Pau, *L'anonymat et le droit*, thèse, Bordeaux IV, 1998.

III. Articles, notes, études

Adam P., Droit (de l'employeur)à la preuve et vie privée(du salarié), *Dalloz*, 2016, p.211.

Ambroise-Castérot C., Recherche et administration des preuves en procédure pénale : la quête du graal de la vérité, *AJ Pénal*, 2005, p.261.

Ambroise-Castérot C., Le FNAEG un outil de fichage au service des enquêtes, *Cahiers, droit sciences et technologies, In*, Le procès pénal à l'épreuve de la génétique, 2019.

Ambroise-Casterot C., Combeau C., La procédure pénale dans la balance : entre secret et transparence, *Les cahiers de la justice*, 2014, p. 373.

Andorno A., Lettre officielle : l'habit ne fait pas le moine, *Dalloz*, 2017, 635.

Allain E., Fichiers d'antécédents : un rapport préoccupant, *AJ Pénal*, 2013, 370.

Apchain H., Retour sur la notion de bonne administration de la justice, *AJDA*, 2012, 587.

Azoulay W., Loyauté de la preuve pénale : un concept de Protée, *Dalloz Actualités*, 17 novembre 2017.

Barrelier A., L'intimité du corps humain comme limite au principe du contradictoire, *Gazette du palais*, 7 novembre 2017, n°38, p. 48.

Bauer D., La vérité en droit : concepts amis ou ennemis ?, *LPA*, n°044, 1er mars 2019, p. 4.

Beaussonie G., La nouvelle garde à vue est elle plus contradictoire ?, *Gazette du palais*, 29 juillet 2014, n°210, p. 13.

Beauvallet O., Les investigations judiciaires internationales, 1ère ed., Berger-Levrault, pages 217 à 219.

Beck J., « L'OCVRP au cœur des ténèbres – Un logiciel qui a fourni ses preuves », Archives du Ministère de l'intérieur, 24 septembre 2015.

Begranger G., Le contrôle des fichiers de police par les juges, *AJ Pénal*, 2014, p. 176.

Belfanti L., *Juge d'instruction*, Répertoire de droit pénal et de procédure pénale, Dalloz, octobre 2015.

Bergeaud-Wetterwald A., Preuve. Du bon usage du principe de loyauté des preuves ? (A propos de l'arrêt rendu par la chambre criminelle de la Cour de cassation le 7 janvier 2014), *Droit pénal*, n°4, avril 2014, étude 7.

Biondo M., Daoud E., Renseignement territorial et fichage un nouveau tour de vis sécuritaire, *AJ Pénal*, 2020, 548.

Bioy X., Les drones produisent-ils des données personnelles ? *AJDA*, 2020, 1552. M.C. Montecler, Il faut une loi sur l'usage des drones par la police, *AJDA*, 2020, 2235.

Blanc N., Gautier PY., Contre « l'anonymisation » des arrêts publiés : décadence des références de jurisprudence, *Dalloz* 2019, p.1648.

Bléry C., *Droit à la preuve : nouvelle pierre à l'édifice jurisprudentiel à propos d'un constat par drone, Dalloz Actualité*, 3 septembre 2019.

Bléry C., Teboul JP., Dématérialisation des procédures : saisine d'une juridiction par le portail du justiciable, *Dalloz actualité*, 5 mars 2020.

Bléry C., Teboul JP., Procédure administrative - Télérecours et télérecours citoyen Apports et perspectives en matière de justice numérique, *JCP G*, 23 novembre 2020, 1330.

Bléry C., Teboul JP., PLINE et PLEX ou les mystères de la nouvelle « communication par voie électronique », *Dalloz actualité*, 18 novembre 2019

Boizard M., Le temps, le droit à l'oubli et le droit à l'effacement, *Les cahiers de la justice*, 2016, p. 619.

Bonis E., Condition de recevabilité d'une demande de réhabilitation judiciaire, *Droit pénal*, n°4, avril 2020, comm.92.

Bonfils P, Gallardo E., *Secret des correspondances*, Répertoire de droit pénal et de procédure pénale, avril 2018, actualisation juin 2018, 119.

Bonnet V., Gouttenoire A., *Divorce, procédure – Exercice de l'action en divorce*, Répertoire de procédure civile, juillet 2017.

Botton A., Le droit à un recours juridictionnel effectif dans le cadre de l'enquête pénale, *Dalloz, Constitutions*, 2014, p. 471.

Bouloc B., Nécessité d'un fait matériel en matière de recel, *RSC*, 1996, p. 645.

Bourgeois M., Moine M., La nouvelle loi informatique et libertés : des changements substantiels après le RGPD, *JCP E*, 5 juillet 2018, n°27.

Bourgeos C., Réflexions à propos de l'anonymisation des décisions de justice publiées sur support numérique, *Communication commerce électronique*, juin 2004, n°6, étude 16.

Bredin JD., « Secret, transparence et démocratie », *in* Pouvoirs, *revue française d'études constitutionnelles et politiques*, avril 2001, n°97p.5-15.

Buat-Ménard E., La justice dite « prédictive » : pré requis, risques et attentes - l'expérience française, *Les cahiers de la justice*, 2019, p. 269.

Buisson J., *Légalité de la preuve*, Répertoire de droit pénal et de procédure pénale, Dalloz, octobre 2020.

Burgorgue-Larsen L., Actualité de la convention européenne des droits de l'Homme, *AJDA*, 2020, p. 160.

Cappello A., Question prioritaire de constitutionnalité, Impact de la question prioritaire de constitutionnalité sur la matière pénale, *Répertoire de droit pénal et de procédure pénale*, n°257, juin 2015, actualisation décembre 2017

Cario R., Ruiz-Vera S., *Victimes d'infractions*, Répertoire de droit pénal et de procédure pénale, juin 2018 actualisation décembre 2020.

Carpentier J., « Neuf ans après les faits, le viol d'une joggeuse enfin élucidé », La voix du Nord, 16 décembre 2016.

Cassar B., La distinction en *l'open data* et l'accès aux décisions de justice, *Dalloz actualité*, 19 juillet 2019.
Cassuto T., La justice à l'épreuve de sa prédictibilité, AJ Pénal, 2017, p. 334.

Catelan N., Arbitrage Tapie-Crédit Lyonnais : relaxe et relaps, *Dalloz actualité*, 26 juin 2019.
Chassard N., Numérisation et communication électronique en matière pénale : quels enjeux, quels apports, quelles contraintes, quelles implications dans la procédure sur le quotidien d'un magistrat du Parquet ? *AJ pénal*, 2014, p.156.

Coustet T., *Open data* judiciaire : le CNB et la Cour de cassation réclament la création d'une instance de régulation, *Dalloz actualité*, 20 mars 2019
Coustet T., Babonneau M., Open data des décisions de justice : le casse-tête judiciaire du 21e siècle, Dalloz actualité, 10 janvier 2018.

Crichton C., Reconnaissance faciale : quels sont les enjeux à prendre en compte ?, *Dalloz Actualité*, 22 novembre 2019.

Crichton C., Création de « DataJust », un algorithme prédictif d'évaluation du préjudice, *Dalloz IP/IT*, 2020, 209.

Chataignier L., Geraud A., Gauthier T., « L'Etat de droit à l'épreuve du renseignement : Bilan du premier rapport d'activité de la CNCTR », *La revue des droits de l'Homme,* février 2017.

Charlent F., Principe du contradictoire et avis de l'avocat général à la Cour de cassation, *Dalloz actualité*, 5 novembre 2019.

Chavagnon A., La protection des sources journalistiques : la décevante loi n°2010-1 du 4 janvier 2010, *Dalloz*, 2010, p. 275.

Chavent-Leclère AS., Procédure pénale – Des évolutions en cours à la révolution attendue en procédure pénale, *Procédures*, 1er janvier 2015.

Chavent-Leclère AS., Rétroactivité du droit à l'effacement du fichier de traitement d'antécédents judiciaires, *Revue procédures*, n°8-9, aout 2018, comm.263.

Dallest J., Le parquet et la communication ou les exigences de la modernité, *AJ Pénal*, 2018, 28.

Danet J., Principe de loyauté des preuves et sonorisation des cellules de garde à vue, *RSC*, 2014, 130.

Daoud E., Jacquin A., L'effectivité du principe du contradictoire, AJ pénal, 2016, p. 112.

Debet A., Données personnelles, droit à l'oubli et droit à l'information du public, *in*, La jurisprudence dans le mouvement de l'open data, *JCP G*, supplément n°9, 27 février 2017, p. 37.

Decima O., De la loyauté de la preuve pénale et de ses composantes, *Dalloz*, 2018, p .103.

Décima O., Terreur et métamorphose, *Recueil Dalloz*, 2016, p. 1826

Delage PJ., Prélèvement sanguin contraint fondé sur l'article 60 du code de procédure pénale : une ingérence « prévue par la loi » ?, *RSC*, 2020, p. 673.

De Leiris E., Becuwe O., N. Touati, N. Palle, Chronique de jurisprudence de la Cour de cassation, *Dalloz*, 2018, p. 757.

De Lamy B., Encadrement constitutionnel des fichiers de police : pas de droit à l'oubli mais un doit à demande l'effacement, *RSC*, 2018, p.993.

Delpech X., Pas de QPC sur le fonds de garantie des dépôts bancaires, *Dalloz actualité*, 19 avril 2012.

Derieux E., Vie privée et données personnelles – droit à la protection et « droit à l'oubli » face à la liberté d'expression, *Nouveaux cahiers du Conseil constitutionnel*, n°48, juin 2015, p.21-33.

Desaulnay O., Ollard R., Le renseignement français n'est plus hors-la-loi. Commentaire de la loi n°2015-912 du 24 juillet 2015 relative au renseignement, *Droit pénal*, n°9, sept. 2015, étude 7.

Desgens-Pasanau G., Le délégué à la protection des données, pierre angulaire du principe de responsabilité, *Communication commerce électronique*, n°4, avril 2018, doss. 6.

Desgens Pasanau G., Droit au déréférencement : nouvelles décisions de la CJUE, de la Cour de cassation et du Conseil d'Etat, *Communication commerce électronique*, n°2 février 2020, étude 3.

Deumier P., Une autre jurisprudence ?, *JCP G*, n°10, 9 mars 2020, doctr. 277.

Dubarry P., « L'obtention des preuves en France et à l'étranger », *Semaine juridique*, édition générale, n°28, 14 juillet 2014, p. 1418.

Du Chaffaut B., Demandes de déréférencement, droit à l'oubli, traitement de données aux fins de journalisme : état des lieux et perspective, *Legipresse*, 2020, p.79.

Eudier F., Gerbay N., *Jugement*, Répertoire de procédure civile, octobre 2018 actualisation décembre 2020, 341.

Favier Y., *Correspondances, messages électroniques*, Répertoire de droit civil, Dalloz, octobre 2019, 103.

Ferrand F., *Preuve. Le juge et les techniques biologiques modernes*, Répertoire de procédure civile, Dalloz, décembre 2013, actualisation décembre 2019.

Ferrand F., *Preuve, Le juge et la preuve écrite*, Répertoire de procédure civile, Dalloz, décembre 2013, actualisation décembre 2019.

Fleuriot C., Géolocalisation : censure partielle pour violation des droits de la défense, *Dalloz actualité*, 27 mars 2014.

Fleuriot C., Expertise médicale et respect du contradictoire, *Dalloz actualité*, 17 juillet 2017.

Fleuriot C., Avec l'accès gratuit à toute la jurisprudence, des magistrats réclament l'anonymat, *Dalloz actualité*, 6 février 2017.

Foret O., Droit à l'oubli des mineurs, *Dalloz IP/IT*, 2018, p.350-352.

F. Fourment, La loi « Renseignement », le renseignement incident de commission d'une infraction et l'autorité judiciaire, *in*, « Le renseignement dans un dossier pénal », *Gazette du palais*, 26 janvier 2016.

Fricero N., Open Data - Diffusion au public et délivrance aux tiers des décisions des juridictions judiciaires Une mise en œuvre responsable et progressive ! , *JCP G*, 13 juillet 2020, 846

Fricero N., Open data des avocats : comment garantir les droits fondamentaux des parties ?, *Procédures*, n 10, octobre 2020, et. 23

Gagnoud P., Le renforcement du contradictoire dans la phase des poursuites : vers une mise en état des affaires pénales ?, *Gazette du palais*, n°214, p. 10

Gaudin V., Roux E., *Coopération policière internationale*, Répertoire de droit pénal et de procédure pénale, octobre 2010, actualisation octobre 2017.

Gautier PY., La prescription sur le billot du contrôle de proportionnalité, *Dalloz*, 2019, p.64.

Gautron V., *Fichiers de police*, Répertoire de droit pénal et de procédure pénale, avril 2015, actualisation mars 2019, 107.

Gautron V., La prolifération incontrôlée des fichiers de police, *AJ Pénal*, 2007 ; 57.

Gautron V., Une mémoire policière hypertrophiée : la fin du droit à l'oubli ?, *Les cahiers de la justice*, 2016, 607.

Giocopelli M., Gallardo E., *Casier judiciaire*, Répertoire de droit pénal et de procédure pénale, septembre 2016, 10 et suivants.

Girault C., Quand la loyauté dicte sa loi, *AJ Pénal*, 2015, p. 362.

Girault C., *Contrôles et vérifications d'identité – Droits et garanties attachés à la rétention aux fins de vérification d'identité*, janvier 2017, Répertoire de droit pénal et de procédure pénale, actualisation mars 2018.

Golhen C., *Facebook* : droit au respect de la vie privée VS droit à la preuve, *Dalloz*, 2020, 2383.

Gouttenoire A., *Mineur*, Répertoire de procédure civile, juin 2015 actualisation décembre 2019, 265.

Guéry C., *Instruction pénale*, Répertoire de droit pénal et de procédure pénale, juin 2018 actualisation novembre 2020.

Guinchard S., *Procès équitable, Garanties procédurales*, Répertoire de procédure civile mars 2017, 521.

Guglielmi GJ., « Comment s'asseoir sur une recommandation de la CNIL. « *Le FIJAIS bouge, il est bien vivant... »*, sur site, www.guglielmi.fr., 9 octobre 2008.

Grayot-Dirx S., La mention « officielle » figurant sur une correspondance entre avocats ne suffit pas pour pouvoir la produire en justice, *JCP G*, n°45, 7 novembre 2016.

Grundler T., Le droit au recours confronté au secret, *AJDA*, 2009, 2358.

Hassier T., Droit de la personnalité, *Recueil Dalloz*, 2007, 2829.

Hauser J., Limites du droit au respect de la vie privée et familiale et droit à la preuve, *RTD civ*. 2012, p. 506.

Hauser J., La preuve biologique, reine des preuves ?, *RTD civ*., 1993, p. 811.

Hauser J., Le droit à l'expertise biologique et la Convention EDH : la vérité biologique à tout moment ?,*RTD civ.* 2011, p. 526.

Hervieu N., « Conventionalité de l'inscription au FIJAIS », *Combats pour les droits de l'homme*, 22 décembre 2009.

Herzog-Evans M., *Réhabilitation*, Répertoire de droit pénal et de procédure pénale, avril 2008, actualisation mars 2018.
Hyde AA., Vers une cyberéthique de la justice « prédictive », *Dalloz IP/IT*, 2019, p. 324.

N. Jacquinot, Le Conseil constitutionnel et le droit à l'oubli en matière de fichiers de police, *JCP Générale*, n°5, 29 janvier 2018, 110
Labayle H., C*oopération judiciaire et policière en matière pénale*, Jurisclasseur Europe, 3 décembre 2017.

Langlois P., Courrier électronique et vie privée au travail, *Dalloz*, 2001, p. 3286.

Larbre D., « Les fichiers de police : une catégorie juridique incertaine ? », *Terminal, technologie de l'information*, culture et société, 108-109, 2011, p. 141 à 151

Lardeux G., *Preuve : règles de preuve – les principes fondamentaux*, Répertoire de droit civil, octobre 2018 points 39 et 380.

Lardeux G., Preuve d'une fraude à l'assurance et respect de la vie privée, *Dalloz*, 2014, p.856.

Larguier J., Le secret de l'instruction et l'article 11 du CPP, *RSC* 1959, 313.

Lavenue JJ., « L'interopérabilité et l'interconnexion des fichiers de police : enjeux et ambiguïté du rapport dialectique entre principe d'efficacité et protection des libertés », *Institut du monde et du développement pour la bonne gouvernance publique IMODEV*, vol. 1, 2014.

Lavric S., *« Fadettes du monde » : violation du secret des sources*, Dalloz actualité 20 décembre 2011.

Lavric S., Recel de violation du secret de l'instruction : quelques rappels, *Dalloz actualité*, 24 juin 2015.

Le Bonniec N., Vers une convergence des exigences constitutionnelles et européennes en matière de protection des données personnelles numériques ?, *JCP G*, n°23, 4 juin 2018, doctr.655.

Leborgne A., L'impact *de la loyauté sur la manifestation de la vérité ou le double visage d'un grand principe*, RTD civ. 1996. 535

Le Calvez J., Les dangers du « X » en procédure pénale : opinion contre le témoin anonyme, *Dalloz*, 2002, p.3024.

Lecourt A., Procédure civile et numérique, *Dalloz IP/IT et communication*, juin 2020.

Meneceur Y., Justice - Open data des décisions de justice Pour une distinction affirmée entre les régimes de publicité et de publication, *JCP E*, 12 septembre 2019, 1415.
Molins F., *Action publique*, Répertoire de droit pénal et de procédure pénale, novembre 2017, actualisation avril 2020.

Mouly J., Témoignages anonymes et droits de la défense du salarié, *Droit social*, 2018, 951.

Le Monnier De Gouville P., La juridictionnalisation de l'enquête pénale, *Les cahiers de la justice, Dalloz*, 2015, n°1, p. 136.

Léna M., Les atteintes liées à l'entrée en vigueur du traitement des antécédents judiciaires, *AJ pénal*, 2013, p. 635.

Léna M, Open data : un équilibre délicat, *AJ pénal*, 2020, p.4
Lepage A., *Droits de la personnalité et nécessité de la preuve*, Répertoire de droit civil, Dalloz, septembre 2009 (actualisé en juillet 2019), n°291.

Lepage A., Des restrictions qui peuvent être apportées à la publicité des débats devant la Cour d'assises, *Communication commerce électronique*, n°5, mai 2019, comm. 33.

Lepage A., Anonymisation des décisions de justice, *Communication commerce électronique*, n°2, février 2002, comm. 29

Leroyer AM., Expertise en matière de filiation : une question d'identité, *RTD civ.*, 2019, p. 305

Lhomond C., Droit à la preuve de l'employeur, loyauté de la preuve et respect de la vie privée « numérique » des salariés une nouvelle articulation, Revue droit du travail, 2020, 764

L'Héritier PH., Ou en est la science de l'hérédité ?, *Revue des deux mondes*, juin 1950, 47, p. 267-285

Loiseau G., Droits de la personnalité, *Légipresse*, 2020, p. 64

Loiseau G., La preuve par Facebook, *JCP G*, 2 novembre 2020, 1226.

Marguénaud JP., *Conv. EDH, art 8 : vie privée,* Répertoire de droit européen, Dalloz, octobre 2017, n°58.

Mauger-Vielpeau L., La filiation paternelle à l'épreuve du contrôle de proportionnalité, *Dalloz*, 2019.

Mayaud Y. « L'état d'urgence récupéré par le droit commun ? Ou de l'état d'urgence à l'état de confusion ! », *JCP G*, 2016, doctr. 344.

Mayaud Y., *Terrorisme, poursuites et indemnisation*, Répertoire de droit pénal et de procédure pénale, Dalloz, janvier 2018, 201.

Marot PY., Fonction et mutation des fichiers de police, *AJ Pénal*, 2007, p. 61.

Mazeaud V., La constitutionnalisation du droit au respect de la vie privée, *Nouveaux cahiers du Conseil constitutionnel*, n°48, juin 2015, p.7-20.

Medjkane M., Le partage des informations à caractère secret, *AJ Pénal*, 2017, p. 371.

Meneceur Y., DataJust face aux défis de l'intelligence artificielle, *JCP G*, 28 septembre 2020, n° 40, doctr. 1087.

Merabet S., « DataJust » et l'effet papillon, *Revue pratique de la prospective et de l'innovation*, octobre 2020, n°2.

Metallinos N., Le principe d'accountability des formalités préalables aux études d'impact sur la vie privée, *Communication commerce électronique*, n°4, avril 2018 , doss. 11.

Mettalinos N., Clarification du Conseil d'Etat sur l'application du droit au déréférencement sur internet, *Communication commerce électronique*, n°2, février 2020, comm.17.

Milano L., Droit d'établir sa filiation biologique et consentement aux tests ADN, *JCP G*, 2011, n°27.

De Montecler MC., Controverse sur l'élargissement des finalités de trois fichiers de police, *AJDA*, 2020, 2398.

Netter E., A quoi sert le principe de transparence en droit des données personnelles ? *Dalloz IP/IT*, 2020, 611.

Nicolas-Gréciano M., Présentation de la législation en matière génétique, *AJ Pénal*, 2018, p. 60

Nicolas-Gréciano M., Présentation de la législation en matière génétique, *AJ Pénal*, 2018, p. 60.

Noguellou R., « Projet de loi relatif au renseignement : le Défenseur des droits exprime ses réserves, *JCP A*, n° 6, juin 2015.

Ollard R., Desaulnay O., La réforme de la législation anti-terroriste ou le règle de l'exception pérenne, *Droit pénal*, n°1, janvier 2015, étude 1.

Parizot R., « Surveiller et prévenir…à quel prix ? Loi n° 2015-812 du 24 juillet 2015 relative au renseignement », *JCP G*, n° 41, 5 oct. 2015, doctr., 1077.

Pastor JM., La CNIL recadre les projets sécuritaires de deux collectivités, *Dalloz Actualité*, 5 novembre 2019.

Pastor J., L'interdiction d'enregistrer les audiences ne méconnait pas la liberté de la presse, *AJDA*, 2019, p. 2521.

Pelletier E., « Dix ans après, le violeur à la montre enfin arrêté », Le parisien, 15 décembre 2016.

Pellier JD., La forme et la force de l'écrit électronique, *Dalloz actualité*, 6 sept. 2018.

Peltier V., Révélation d'une information à caractère secret, *JurisClasseur pénal*, Fasc. 30, 28 mai 2015.

Perrocheau Y., Les fluctuations du principe de loyauté dans la recherche des preuves, *LPA*, 2002, n° 99, p. 6.
Pettiti LE., Principe du contradictoire et égalité des armes, *RSC*, 1992, p. 798.

Prétot X., Sécurité sociale, contentieux de la sécurité sociale, expertise médicale, communication du rapport d'expertise, principe du contradictoire, *Dalloz social,* 2001, p. 576.

Priou-Alibert L., Infraction sexuelle : consécration de l'automaticité de l'inscription au fichier, *Dalloz actualité,* 24 mars 2010.

Puydebois G., Le pas mesuré de la Cour européenne des droits de l'Homme vers la reconnaissance d'un droit d'accès à l'information, *Revue JADE,* 1 janvier 2017

Py B., *Secret professionnel*, Revue de droit pénal et de procédure pénale, Février 2003, actualisé mai 2020, 95.

Py B., Secret professionnel : le syndrome des assignats ?, *AJ pénal*, 2004, p. 133.

Py B., *Amnistie*, Répertoire de droit pénal et de procédure pénale, octobre 2003, actualisation juin 2012.

Quéméner M., Les nouvelles dispositions de lutte contre la cybercriminalité issues de la loi du 13 novembre 2014 renforçant la lutte contre le terrorisme, *AJ Pénal*, 2015, p. 32

Quéméner M., La preuve numérique dans un cadre pénal, *Jurisclasseur communication*, n° 1105 avril 2019.

Quéméner M., La preuve numérique pénale à l'épreuve de la déloyauté, *Actualités du droit, Lamyline*, 27 août 2019.

Quéméner M., Le refus de déchiffrement à l'épreuve des droits fondamentaux, Dalloz IP/IT, 2018, p. 514.

Rayne S., *Perquisitions – saisies – visites domiciliaires*, Répertoire de droit pénal et de procédure pénale, Dalloz, octobre 2008, actualisé en février 2018, 27 - 40.

Redon M., *Tribunal correctionnel*, Répertoire de droit pénal et de procédure pénale, juin 2017 actualisation novembre 2020

Renneville M., L'affaire Joseph Vacher : la fin d'un brevet d'impunité » pour les criminels ?, *Droit et cultures*, février 2010, p. 129-142.

Renucci JF., Loyauté des preuves et distinction entre « provocation à l'infraction » et « provocation à la preuve », *RSC,* 2014, p.843.

Riccardi C., Richefeu L., Les nouvelles utilisations de la génétique dans le cadre de la procédure pénale, *RSC*, 2018, p. 331.

Rivollier V., L'open data des décisions de justice : pas tout, pas tout de suite, *Dalloz,* 2020, p.1626.
J.H. Robert, *Administration judiciaire de la preuve*, JurisClasseur Procédure civile, Fasc. 700-12, 2 janvier 2017

Roblet-Troizier A. *in Les nouveaux cahiers du Conseil constitutionnel*, n°40, 2013.

Rotily C., Archambault L., Drones civils professionnels et RGPD : enjeux liés à la collecte des données personnelles et au respect de la vie privée, *Dalloz IP/IT*, 2019, 376.

Rotily C., L. Archambault, Données biométriques issues d'expérimentations de reconnaissance faciale sur le territoire français : un défi à l'aune du droit 2.0 ? *Dalloz* IP/IT, 2020, p. 54.
Rubi-Cavagna E., L'extension des procédures dérogatoires, *RSC*, 2008, p. 23.

Saint Pau JC., Droit à la preuve versus droit au respect de la vie privée, *Dalloz* 2016, p.884.

Saint-Pau JC., Le ministère public concurrence-t-il le juge du siège ?, *Droit pénal*, n° 9, septembre 2007, et. 14.

Saulier M., Droit à une filiation vs droit au respect de la vie privée du père : y a-t-il vraiment encore un débat ?, *AJ Famille*, 2019, p. 155.

Serre C., Evrard C., Du rififi chez les grandes oreilles, Etude sur les enjeux des interceptions judiciaires dans la procédure pénale au prisme de la plateforme nationale des interceptions judiciaires, Dalloz Actualité, 4 février 2020.

Sicilianos LA., Kostopoulou MA., *Conv. E.D.H. art. 6 : la protection du droit à un procès équitable dans la jurisprudence de la Cour européenne des droits de l'homme*, Répertoire de droit européen, janvier 2018 actualisation février 2020, 97, 98.

Schwendener M., *Police technique et scientifique*, Répertoire de droit pénal et de procédure pénale, octobre 2016 actualisation février 2019.
Sztejnhorn C., L'open access et l'édition juridique : l'exemple de la disruption open Dalloz, *Dalloz IP/IT*, 2017,p.97.

Tambou O., Que retenir du projet de loi relatif à la protection des données personnelles ? Partie II : l'amélioration relative du régime des traitements pénaux par la transposition de la directive n°2016/680, RLDI 2018/146, 1er mars 2018,

Tixier G., A.G. Hamonic-Gaux, Portée du droit de communication de l'administration fiscale et compatibilité des arrêts de la Cour européenne des droits de l'homme et des arrêts du Conseil d'Etat, *Dalloz*, 1998, p. 159.

Thierry G., Comment le ministère de la justice espère rebondir sur le dossier des écoutes judiciaires, Dalloz actualité, 21 novembre 2018.

Türk P., L'autodétermination informationnelle : un droit fondamental émergent ?, *Dalloz IP/IT*, 2020, 616

Umberto Gout E., Le sort des pièces de la procédure pénale devant le juge civil, *LPA*, 7 décembre 2018, n 245, p. 6.

Vauthier JP., Expertise médicale et intimité de la victime : l'absence de l'auteur aux opérations d'expertise ne porte pas atteinte au principe du contradictoire, *RDS*, 2017, n°80, p.814-815.

Vergès E., La réforme du droit de la preuve civile : enjeux et écueils d'une occasion à ne pas manquer, *Dalloz*, 2014, p. 617

Viganotti E., Filiation : deux décisions intéressantes de la CEDH, *AJ Famille*, 2014, p. 246.

Yazici MH., Conformité constitutionnelle du huis clos de droit à la demande de la partie civile, *Dalloz Actualité*, 13 septembre 2017

IV. Avis, Rapports, Délibérations

Délibérations, Avis CNIL

Délibération CNIL n°82-199 du 30 novembre 1982 portant avis sur la mise en œuvre du fichier informatisé des personnes par la direction centrale des renseignements généraux du Ministère de l'Intérieur et de la Décentralisation. La CNIL s'est rarement prononcée sur les fichiers relatifs aux services de renseignements avant le décret du 14 octobre 1991 les rendant « officiels ».

Délibération CNIL n°86-102 du 14 octobre 1986 concernant un projet de décret relatif au fichier automatisé des empreintes digitales géré par le Ministère de l'Intérieur.

Délibération CNIL, n°95-012 du 24 janvier 1995 portant recommandation relative aux données personnelles traitées ou utilisées par des organismes de la presse écrite ou audiovisuelle à des fins journalistiques et rédactionnelles

Délibération CNIL 2006-066 du 16 mars 2006 portant adoption d'une recommandation relative à la mise en œuvre de dispositifs destinés à géolocaliser les véhicules automobiles utilisés par les employés d'un organisme privé ou public.

Délibération CNIL n°2007-110 du 24 mai 2007 portant avis sur un projet de décret pris pour l'application du deuxième alinéa de l'article L. 611-3 du code de l'entrée et du séjour des étrangers et du droit d'asile portant création d'un traitement automatisé de données à caractère personnel des ressortissants étrangers faisant l'objet d'une mesure d'éloignement et modifiant la partie réglementaire de ce même code.

Délibération CNIL n°2007-326 du 8 novembre 2007 relative au projet de décret n°2008-1023 du 6 octobre 2008 relatif au FIJAIS.

Rapport CNIL du 20 janvier 2009, conclusions du contrôle du système de traitement des infractions constatées.

Délibération CNIL n°2009-356 du 11 juin 2009 portant avis sur un projet de décret en Conseil d'Etat portant création de l'application concernant les enquêtes administratives liées à la sécurité publique.

Délibération CNIL n°209-587 du 12 novembre 2009 portant avis sur un projet de décret en Conseil d'Etat relatif au fichier des personnes recherchées (FPR).

Délibération CNIL n° 2011-418 du 15 décembre 2011 portant avis sur un projet de décret relatif à la mise en œuvre de logiciels de rapprochement judiciaire à des fins d'analyse criminelle (demande d'avis n° 1523917).

Délibération n° 2012-321 du 20 septembre 2012 portant avis sur projet de décret relatif à la mise en œuvre de fichiers d'analyse sérielle dénommés « bases d'analyse sérielle de police judiciaire » (demande d'avis n° 12012464).

Décision CNIL 2012-365 du 11 octobre 2012 portant avis sur un projet de décret relatif modifiant le décret n° 2011-110 du 27 janvier 2011 portant création d'un traitement automatisé de données à caractère personnel dénommé LRPPN 2. Demande d'avis n° 12017917.

Rapport CNIL du 13 juin 2013 adopté en assemblée plénière relatif au contrôle des fichiers d'antécédents du ministère de l'intérieur

Délibération n° 2014-009 du 16 janvier 2014 portant avis sur un projet de décret autorisant la mise en œuvre d'un traitement automatisé de données à caractère personnel dénommé « Plate-forme nationale des interceptions judiciaires ».

Délibération CNIL n°2015-078 du 5 mars 2015 portant avis sur un projet de loi relatif au renseignement.

Délibération CNIL n°2015-119 du 7 avril 2015 portant avis sur un projet de dispositions législatives visant à créer un fichier national des auteurs d'infractions terroristes (FIJAIT), rendu public sur demande du Gouvernement.

Délibération n°2017-153 du 18 mai 2017 portant avis sur un projet de décret modifiant plusieurs traitements automatisés de données à caractère personnel du code de la sécurité intérieure.

Délibération CNIL SAN-2021-003 du 12 janvier 2021

Délibération CNIL n° 2020-002 du 9 janvier 2020 portant avis sur un projet de décret en Conseil d'Etat portant création d'un traitement automatisé de données à caractère personnel dénommé « DataJust » (demande d'avis n° 19020148).

Délibération CNIL n°2020-036 du 12 mars 2020 portant avis sur un projet de décret portant création d'un traitement automatisé de données à caractère personnel dénommé « dossier pénal numérique ».

Délibération CNIL n° 2020-065 du 25 juin 2020 portant avis sur un projet de décret modifiant les dispositions du code de la sécurité intérieure relatives au traitement de données à caractère personnel dénommé « Gestion de l'information et Prévention des atteintes à la sécurité publique » (demande d'avis n° 19013314)

Délibération CNIL n° 2021-011 du 26 janvier 2021 portant avis sur une proposition de loi relative à la sécurité globale (demande d'avis 20020769).

Rapports

A.E. Credeville, *Vérité et loyauté des preuves*, Rapport 2004, Cour de cassation.

S. Goy-Chavent, *Menace terroriste, pour une République juste mais plus ferme,* Rapport de la Commission d'enquête déposé le 4 juillet 2018.

Rapport du Parlement européen, *« Les conséquences de l'usage civil des drones sur la protection de la vie privée et des données à caractère personnel »*, 2015.

Rapport de la Cour de cassation, P. Lemoine, La loyauté de la preuve à travers quelques arrêts récents de la chambre criminelle, 2004.

F. Agostini, N. Molfessis, Rapport, *Amélioration et simplification de la procédure civile*, Chantiers de la justice, référents, janvier 2018, proposition 23, p. 30 et s.

L. Viard-Guillot, Le traitement judiciaire des infractions liées aux stupéfiants en 2015, *Bulletin d'informations statistiques du ministère de la Justice*, mars 2017, n° 150, p. 2.
A. Bauer, C. Soullez, M. Ventre, *Mieux contrôler la mise en œuvre des dispositifs pour mieux protéger les libertés,* La documentation française, coll. Des Rapports officiels, 2008, p.15

Rapport d'information de la commission des lois constitutionnelles, de la législation et de l'administration générale de la République sur les fichiers de police, Députés BATHO D. et BENISTI J-A, déposé le 24 mars 2009.

J. Richard, Rapport public du référent national, *Traitement de données à caractère personnel « Gestion de l'information et de la prévention des atteintes à la sécurité publique » de la Gendarmerie nationale en ce qu'il concerne les mineurs*, mai 2018.

Rapport d'information de la commission des lois constitutionnelles, de la législation et de l'administration générale de la République sur les fichiers mis à la disposition des forces de sécurité, Députés Paris D. et Morel-A-L'Huissier P., déposé le 17 octobre 2018.

Rapport du groupe de diagnostic stratégique n°6, 25e session nationale « Sécurité et Justice », 2013/2014, « Fichiers de police et libertés : des enjeux nationaux, une nouvelle donne internationale », janvier 2015.

Institut National des hautes études de la sécurité et de la justice, « Fichiers de police et libertés : des enjeux nationaux, une nouvelle donne internationale », Travaux des auditeurs, Rapport du Groupe de diagnostic stratégique n°6 – 25e Session nationale « Sécurité et Justice » - 2013/2014.

Rapport de la commission des lois, n°2540, 18 décembre 2019, le secret de l'enquête et de l'instruction.

Rapport du comité de réflexion sur la justice pénale déposé le 1er septembre 2010.

Pré- Rapport du comité de réflexion sur la justice pénale déposé 6 mars 2009.

J. Beaumes, *Rapport sur la procédure pénale*, juillet 2014

L. Cadiet, Rapport sur l'open data des décisions de justice, novembre 2017.

Rapport Braibant, Données personnelles et société de l'information, 3 mars 1998, p.7.

E. Lesueur De Givry, *La question de l'anonymisation des décisions de justice*, *in,* Rapport annuel de la Cour de cassation, 2000, Doc. Fr., 2000

Rapport annuel d'activité CNIL 2019.

Boizard M. (dir.), Blandin A., Corgas C, Dedessus Le Moustier G., Gambs S., Lejealle C, Moisdon-Chataigner S., Pierre P.,Piolle G., Rousvoal L., *Le droit à l'oubli*, Mission de recherche Droit et Justice, févr. 2015.

Avis du groupe « article 29, n°2/2009 sur la protection des données à caractère personnel de l'enfant, 11 février 2009.

Rapport du Conseil d'État, *Le numérique et les droits fondamentaux*, 2014.

Actes de colloques

Clément-Fontaine M., colloque relatif à la preuve numérique à l'épreuve du litige, Compagnie nationale des experts de justice en informatique et techniques associées, 13 avril 2010.

Fourre P., *La judiciarisation du renseignement*, Colloque sur « Le renseignement de sécurité et de défense », Forum de recherche de l'AFDSP, 25 juin 2020.

Hurel B., *Les difficultés relatives à la judiciarisation*, Colloque sur « Le renseignement au service de l'enquête », Institut national des hautes études de la sécurité et de la justice, 21 mai 2019.

Serge Migayron M., lors d'un colloque relatif à la preuve numérique, Colloque, La preuve numérique à l'épreuve du litige, Cour d'appel de Paris, 13 avril 2010.

INDEX

(*Les chiffres renvoient aux paragraphes*)

A

ADN
V. *Preuve*
Analyse sérielle : 243 s.
Anonymat : 329
Anonymisation : 360, 420, 421

C

Casier judiciaire national : 486, 492, 497 s.
Coopération judiciaire et policière : 255 s.

D

Dématérialisation des procédures : 384 s.
Déréférencement (droit au) : 473 s.
Donnée à caractère personnel :
- Confidentielle : 324 s.
- Conservation : 293
- Interconnexion : 446, 501

Drones : 64

E

Effacement (droit d') : 478.
Enquête (secret de l') : 298 s.
Enquête sous pseudonyme : 49

F

Fichiers des personnes recherchées : 183 s.
Fichier national des empreintes digitales : 172 s., 209
Fichiers national des empreintes génétiques : 180 s.

G

Géolocalisation : 30

H

Huis-clos : 333

I

IMSI-catcher : 45
Instruction (secret de l') : 298 s.
Interceptions de données : 43 s.

L

Légalité
V. *Preuve*
Loyauté
V. *Preuve*

M

Mandat européen : 37

O

Open access : 412 s.
Open data : 412 s.
Oubli (droit à) : 461 s.

P

Prélèvement biologiques : 73
Preuve :
- ADN : 74, 119 s.
- Légalité (de la) : 23 s.
- Loyauté (de la) : 76 s.
- Numérique : 126 s.

Pseudonymisation : 427 s
Publicité (principe de) : 296, 332

R

Rectification (droit de) : 294

S

Secret professionnel : 303 s.
Secret de l'enquête
V. *Enquête*
Secret de l'instruction
V. *Instruction*
Sonorisation : 47

T

Traitement des antécédents judiciaires : 163 s.

TABLE DES MATIERES

SOMMAIRE..... 1

INTRODUCTION.....3

PREMIERE PARTIE
L'EXPLOITATION DES DONNEES A CARACTERE PERSONNEL DANS LES PROCEDURES JUDICIAIRES 19

TITRE 1 : Les données à caractère personnel intervenant dans les procédures judiciaires à titre probatoire..... 21

Chapitre 1 : La collecte des données à caractère personnel au regard des principes encadrant la licéité de la preuve.....25
Section 1 : La collecte de données probatoires soumise au principe de licéité de la preuve.....26
§1. Le respect de la légalité formelle 27
A. La réglementation générale des actes d'enquête 28
1° Les données collectées sur réquisition judiciaires 28
2° Les données collectées par perquisition ou saisie.....29
3° Les données interceptées 30
4° Les données collectées par le recours aux expertises 32
5° Les procédés de collecte de données à vocation probatoire à l'étranger 33
a. La collecte de preuves civiles et commerciales à l'étranger 33
b. La collecte de preuves pénales à l'étranger.....36
B. La collecte de données probatoires relevant de procédés dérogatoires.....36
1° Le régime des interceptions de données relevant largement d'un régime dérogatoire.....38
2° La collecte de données probatoires facilitée par le recours à des procédés dérogatoires.....40
C. La collecte de données judiciaires auprès des services de renseignement : la judiciarisation du renseignement.....43
1° Le constat préalable de l'augmentation des pouvoirs octroyés à la police administrative 44
2° Le recours au données probatoires issues du renseignement.....47
§2. Le respect de la légalité matérielle.....49
A. La collecte de données personnelles à vocation probatoire confrontée au principe du respect de la vie privée 50
1° L'application du principe de légalité en matière de production de correspondances 50
2° Le principe de légalité en matière de captation d'images.....52
3° La légalité dans la collecte de preuves dans l'entreprise 55
B. La collecte de données personnelles à vocation probatoire confrontée au principe de sauvegarde de la dignité humaine.....59
1° La prohibition de toute atteinte à la dignité humaine dans la collecte de données à vocation probatoire 60
2° Réflexion quant à la place du consentement dans la collecte de données probatoires.....61

Section 2 : La collecte de données soumise au principe de loyauté de la preuve.....65
§1. Le principe de loyauté dans la collecte de preuves 67
A. Portée ambivalente du principe de loyauté de la preuve 67
1° L'absence de définition de la loyauté 67
2° Une construction jurisprudentielle et doctrinale d'un principe ambivalent.....68
B. Une application distincte du principe de loyauté en fonction du contentieux.....69
1° L'application du principe de loyauté en matière civile 69
2° L'application du principe de loyauté en matière pénale 70
§2. L'application du principe de loyauté dans la collecte de données à caractère personnel.....72
A. La collecte loyale de données à caractère personnel en matière civile 73
1° La loyauté dans la collecte de données informatiques.....73
2° La loyauté dans la collecte de données par l'usage de dispositifs de surveillance.....74
B. La collecte loyale de données à caractère personnel en matière pénale.....75
1° La loyauté dans la collecte de données informatiques.....75
2° La loyauté dans la captation de données en temps réel 77

Chapitre 2 : L'impact de la nature particulière des données à caractère personnel sur leur fonction probatoire.....79
Section 1 : La collecte de données à caractère personnel au regard de leur nature 80
§1. La collecte de données à caractère personnel soumises au secret.....
A. La collecte de données soumises au secret professionnel 80
B. La collecte de données face au secret des sources 83
§2. La collecte de données à caractère personnel numériques.....84
A. Les réquisitions portant sur des données numériques 85
B. Le cas particulier de l'accès aux données chiffrées.....85
Section 2 : L'impact de la nature des données dans l'appréciation de la preuve.....87
§1. La valeur probante des données scientifiques.....89
A. De la donnée scientifique à la preuve juridique 89
1° La preuve par les données génétiques.....90
2° Le portrait robot génétique 93
B. Les potentielles évolutions quant au recours aux données biométriques dans le procès 94
§2. La valeur probante des données numériques.....96
A. L'appréciation de la preuve encadrée par la loi.....96
B. L'appréciation de la donnée numérique 98
Conclusion du titre 1 99

TITRE 2 : Les données à caractère personnel alimentant des fichiers judiciaires 101

Chapitre1 : La création des fichiers judiciaires 109
Section 1 : Les critères fonctionnels justifiant la création de fichiers judiciaires 110
§1. La prévention des infractions par les fichiers à vocation judiciaire et de renseignement.....112
A. Les fichiers à vocation judiciaire.....112
1° Le répertoire des données à caractère personnel collectées dans le cadre de procédures judiciaires (REDEX).....113
2° La plateforme judiciaire des interceptions judiciaires 115

B. Les fichiers de renseignement 117
§2. La constatation d'infractions et le recueil de preuves facilités par les fichiers d'antécédents judiciaires 122
A. Historique de la création du STIC et du JUDEX 123
B. La fusion du STIC et du JUDEX portant création du TAJ 125
1° Les motivations de la fusion STIC/JUDEX 125
2° Les nouvelles garanties apportées 128
§3. L'identification des individus par le biais de données génétiques et biométriques 128
A. L'identification par les empreintes digitales 129
B. L'identification par le fichage des auteurs d'infractions 131
1° Le fichier automatisé des auteurs d'infractions sexuelles ou violentes 131
2° Le fichier judiciaire automatisé des auteurs d'infractions terroristes 131
C. L'identification par l'ADN 136
D. Le fichier des personnes recherchées 139
§4. Le cas particulier du casier judiciaire national, véritable mémoire judiciaire 141
§5. Les traitements de données judiciaires au service de la prédictivité de la justice 145
A. Enjeux de la justice prédictive en termes de traitement de données à caractère personnel 145
B. « DataJust » prémisses de la justice prédictive 147
1° Le décret portant création de « DataJust » 147
2° Interrogations soulevées quant à la concrétisation de l'usage des algorithmes en matière judiciaire 148
Section 2 : Le cadre réglementaire relatif aux fichiers judiciaires 151
§1. La loi informatique et libertés 151
A. Le rôle de la CNIL en matière de création de fichiers 152
1° Un allègement des prérogatives a priori par la suppression des formalités préalables à la mise en œuvre de traitements 153
2° Le régime d'avis 154
B. Le maintien résiduel d'un régime d'autorisation 158
1° Le traitement de données sensibles soumis à autorisation du Conseil d'Etat 158
2° La reprise et l'accentuation des dispositions de la directive Police-Justice en matière de traitement de données pénales 159
3° Le renforcement des obligations incombant au responsable du traitement 159
§2. Le contrôle de légalité opéré par le Conseil d'Etat 160
§3. Le contrôle de constitutionnalité 161
A. Le contrôle a priori des lois portant créations de fichiers judiciaires 165
1° Validation par le Conseil constitutionnel 165
2° Censure du Conseil constitutionnel 167
B. Le contrôle a posteriori des lois portant création de fichiers judiciaires 168
§4. Le contrôle des juges supranationaux 171
Chapitre 2 : Le partage de données fichées 171
Section 1 : Le partage de données à caractère personnel au niveau national 173
§1. Le rapprochement de données judiciaires 174
A. Les outils d'analyse sérielle 174
B. Les logiciels de rapprochement judiciaire 178
§2. L'interconnexion entre fichiers judiciaires nationaux 186
A. L'interconnexion outil de fiabilité et d'efficacité 182
B. L'interconnexion et les risques pour les libertés individuelles 183
Section 2 : Le partage de données à caractère personnel au niveau international dans le cadre de la coopération judiciaire et policière 185

§1. Le cadre structurel et institutionnel de la coopération judiciaire et policière 186
A. Le partage de données à caractère personnel dans le cadre de l'acquis Schengen 187
1° Le cadre de mise en œuvre de la surveillance des frontières extérieures 187
2° Le partage de données dans le cadre du renforcement de la coopération policière et judiciaire 190
B. Le partage de données à caractère personnel avec les Etats n'adhérant pas à Schengen 192
C. Le partage de données à caractère personnel dans la cadre de la coopération renforcée dans l'espace de liberté, de sécurité et de justice 195
§2. Les acteurs de la coopération policière et judiciaire 198
A. Les acteurs de la coopération judicaire 198
1° Les acteurs du partage de données dans la cadre de la coopération judiciaire 199
2° L'unité chargée du renforcement de la coopération judiciaire en Europe Eurojust200
B. Les acteurs de la coopération policière 204
1° Les acteurs nationaux de coopération policière 205
2° Les organismes internationaux de coopération policière 207
Conclusion du titre 2 211
Conclusion de la partie 1 213

DEUXIEME PARTIE
LA PROTECTION DES DONNEES A CARACTERE PERSONNEL DANS LES PROCEDURES JUDICIAIRES 217

TITRE 1 : Les principes encadrant la diffusion des données à caractère personnel au cours de la procédure judiciaire 219

Chapitre 1 : Les principes limitant la diffusion de données 221
Section 1 : Un secret affirmé lors de la phase d'enquête et d'instruction 221
§1. Le secret protégeant les données de l'enquête et de l'instruction 222
A. L'affirmation d'un principe protecteur des données 222
B. Une portée limitée du principe du secret de l'enquête et de l'instruction 224
1° Un principe non absolu 224
2° La nécessaire communication des données du dossier aux parties 227
§2. Le secret partagé applicable aux données des procédures judiciaires 233
A. Le partage de dossier entre magistrats 234
B. Le partage de dossiers judiciaires avec l'Administration 235
§3. La communication illégale de données issues de procédures d'enquête et d'instruction 237
Section 2 : Une confidentialité relative lors de la phase de jugement 242
§1. La protection directe attachée au caractère confidentiel des données 242
A. L'interdiction de communiquer des données couvertes par un secret professionnel 242
1° La caractère relatif ou absolu du secret 243
2° L'application stricte du principe de secret 244
B. La protection par l'anonymisation du témoignage 246
§2. La protection indirecte résultant de l'absence de publicité 248
A. Les débats tenus non publiquement 248
1° L'exception à la publicité en cas de menace pour l'ordre public 249
2° L'exception à la publicité en cas de menace pour les intérêts privés 249

3° L'exception à la publicité attachée à la nature du contentieux 250
B. Les jugements rendus non publiquement 251
Chapitre 2 : Les principes justifiant la diffusion de données 253
Section 1 : La diffusion de données découlant de l'application de principes généraux 253
§1. Les données communiquées par l'application du contradictoire 253
A. La portée du principe de la contradiction 254
1° Un droit naturel 254
2° Le contradictoire comme affirmation d'un droit à l'information 256
B. Le sort des données à caractère personnel dans l'application du principe du contradictoire dans le cadre d'expertises 260
§2. Les données diffusées par l'application du principe de publicité 263
A. Les données du débat rendues publiques 264
1° La portée du principe de publicité des débats 264
2° La diffusion des données du débat par reproduction dans la presse 265
B. Les donnés du jugement rendues publiques 268
Section 2 : Une approche extensive de la diffusion des données 269
§1. La nécessaire communication de donnés protégées 270
A. La divulgation de données d'enquête et d'instruction 270
1° La divulgation de données secrètes sous couvert de protection de l'ordre public 270
2° La communication des données secrètes nécessaires dans une instance civile 272
a° La communication de données de procédures entre juridictions pénales et civiles 272
b° La production par les parties dans une instance civile de données issues d'une instruction en cours 273
B. La communication de données couvertes par un secret professionnel 275
1° Le choix de communiquer des données couvertes par un secret 276
a° « L'option de conscience » du professionnel détenteur du secret 277
b° La production de correspondances privées 279
c. La communication par une partie dépositaire de données couvertes par le secret afin d'assurer sa défense 280
2° L'obligation de communiquer des données couvertes par un secret 280
a° L'obligation de divulguer la donnée secrète en cas de péril pour la personne 281
b° Le détenteur du secret appelé à déposer en sa qualité d'expert 282
c° Le dépositaire d'un secret appelé à révéler les données en tant que détenteur de données utiles à l'autorité judiciaire 284
d° Le dépositaire appelé à s'exprimer du fait de sa qualité de partie 285
§2. La diffusion des données de procédure facilitée par la dématérialisation 287
A. La mise en œuvre d'un traitement dématérialisé des donnés de procédure 288
1° Les prémisses de la dématérialisation des procédures judiciaires 289
2° La mise en œuvre de la dématérialisation en matière civile 290
3° La mise en œuvre de la dématérialisation en matière pénale 293
B. La protection des données à caractère personnel dans une procédure
C. dématérialisée 295
1° La protection prévue par les textes 296
2° Le recours nécessaire à des outils sécurisés 297
3° Le traitement dématérialisé des données protégées 299
Conclusion du titre 1 299

TITRE 2 Le sort des données à caractère personnel collectées dans le cadre de procédures judiciaires 303

Chapitre 1 : La gestion de données à caractère personnel collectées dans le cadre d'une procédure judiciaire 305
Section 1 : L'encadrement de la diffusion des décisions de justice 305
§1. La mise à disposition numérique des décisions de justice 306
A. La consécration d'un droit d'accès numérique aux données judiciaires 307
1° Une distinction affirmée entre *open access* et *open data* 307
2° La multiplication des modes de diffusion des décisions de justice 310
B. La mise à disposition des décisions de justice au regard des normes encadrant le traitement de données à caractère personnel 311
1° La mise à disposition des décisions au regard du principe de licéité du traitement 312
2° La mise à disposition des décisions au regard des droits des individus visés par le traitement 314
§2. La protection des données à caractère personnel contenues dans les décisions de justice diffusées 316
A. La protection des données à caractère personnel par l'anonymisation des décisions de justice 317
B. La protection des données à caractère personnel contenues dans les décisions de justice par la pseudonymisation 321
C. Le régime de protection des données initié par la loi du 23 mars 2019 323
1° La protection des données à caractère personnel dans l'accès aux décisions 323
2° La protection des données à caractère personnel contenues dans les jugements diffusés en open data 324
Section 2 : La gestion des données à caractère personnel fichées 326
§1. Les normes encadrant la gestion des données à caractère personnel fichées 326
A. Les normes encadrant la gestion des fichiers judiciaires 326
1° Les durées légales de conservation des données contenues dans les fichiers de police 327
2° Les normes régissant le transfert des données fichées 329
B. Les faits justifiant une rectification ou un effacement de droit des données fichées 331
1° L'effacement d'office fondé sur le critère de finalité du traitement 331
2° La mise à jour des données fichées 333
§2. Les droits des individus quant à la gestion de leurs données à caractère personnel fichées 334
A. L'absence de droit d'opposition au traitement de données en matière judiciaire 334
B. Le droit d'accès aux données fichées lors de procédures judiciaires 335
1° L'étendue du droit d'accès 335
2° L'application du droit d'accès aux données contenues dans les fichiers judiciaires 336
a° L'accès direct aux données fichées 337
b° L'accès indirect aux données fichées 337
C. Les sanctions du non respect des droits des individus quant au traitement de leurs données à caractère personnel 339
1° Le pouvoir de sanction de la CNIL 339
2° La méconnaissance des droits des individus constitutive d'infractions pénales 341

Chapitre 2 : Le droit à l'oubli des données à caractère personnel collectées dans le cadre d'une procédure judiciaire 343

Section 1 : De l'émergence du droit à l'oubli à la reconnaissance d'un droit à l'effacement des données 344
§1. La reconnaissance progressive d'un droit à l'oubli 344
A. La reconnaissance jurisprudentielle du droit à l'oubli 345
1° L'émergence de la notion d'oubli dans le droit 345
2° La reconnaissance jurisprudentielle du droit à l'oubli 346
B. La reconnaissance d'un droit à l'oubli numérique par l'affirmation du droit à l'effacement de données pour motifs légitimes 347
1° L'émergence d'un droit à l'oubli numérique 348
2° La reconnaissance d'un droit au déréférencement 350
3° La consécration d'un droit à l'effacement des données pour motifs légitimes par le droit européen 352
§2. Le droit à l'oubli appliqué aux données traitées au cours de procédures judiciaires 355
A. L'oubli attaché au critère de temps 355
B. L'oubli comme principe protecteur des droits des individus 357
1° L'oubli découlant de l'issue des poursuites 357
2° Les requêtes en effacement anticipé des données fichées 358
Section 2 : L'effectivité du droit à l'oubli s'agissant des données à caractère personnel intervenant lors de procédures judiciaires 361
§1. Le droit d'être oublié de la mémoire judiciaire : un droit relatif 362
A. La nécessaire conservation des données : la mémoire judiciaire 363
1° La nécessaire conservation des données à vocation judiciaire au sein de fichiers judiciaires 363
2° La nécessaire conservation des données relatives aux condamnations au sein du casier judiciaire national 364
B. Les limites du droit à l'oubli s'agissant des données faisant l'objet d'un fichage par les autorités 367
1° Les limites du droit à l'oubli conséquence des dispositions légales encadrant la gestion des données fichées 367
2° Les limites du droit à l'oubli conséquence du traitement massif des données judiciaires 369
§2. Le droit d'être oublié de la mémoire collective : un droit émergent mais limité 370
A. Les problématiques liées à la rediffusion des données du procès 371
1° Un droit au déréférencement limité 371
2° Une anonymisation des données insuffisante à assurer l'effectivité d'un droit à l'oubli 374
B. L'effectivité d'un réel droit à l'oubli s'agissant de son passé judiciaire 376
1° L'émergence de notions relatives à l'oubli 376
2° La conceptualisation de l'oubli 377
Conclusion du titre 2 378
Conclusion de la deuxième partie 381
Conclusion générale 383
Bibliographie 387
Index 405