Les investigations numériques en procédure pénale

Bruno Roussel

université de BORDEAUX

THÈSE PRÉSENTÉE
POUR OBTENIR LE GRADE DE

DOCTEUR DE L'UNIVERSITÉ DE BORDEAUX

ÉCOLE DOCTORALE DE DROIT
SPÉCIALITÉ DROIT PRIVE ET SCIENCES CRIMINELLES

Par Bruno ROUSSEL

Les investigations numériques en procédure pénale

Sous la direction de Monsieur le Professeur Olivier DÉCIMA
et de Monsieur Fabrice PEYRARD

Soutenue le 7 juillet 2020

Membres du jury :

Madame le Professeur Coralie AMBROISE CASTÉROT,
Professeur à l'Université de Nice-Sophia Antipolis, ***rapporteur, Présidente du jury***

Monsieur le Professeur Édouard VERNY
Professeur à l'Université Paris 2 Panthéon-Assas, ***rapporteur***

Monsieur le Professeur Olivier DÉCIMA,
Professeur à l'Université de Bordeaux, ***directeur de thèse***

Monsieur Fabrice PEYRARD,
Maître de conférences HDR à l'IUT de Blagnac, ***co-directeur de thèse***

A Vanessa et Chloé
pour leur soutien indéfectible
et pour m'avoir donné la force
d'aller jusqu'au bout,
malgré les nombreuses conséquences
que cette formation a pu avoir sur notre vie de famille.

REMERCIEMENTS

A l'heure de mettre un point final aux présents travaux, qui auront été, pour moi, d'une richesse, non seulement scientifique, académique, mais également humaine extraordinaire, mes premières pensées se tournent vers mes deux directeurs de thèses, le Professeur Olivier DECIMA et Fabrice PEYRARD, Maître de conférences HDR en informatique. Leur patience et la qualité de leur accompagnement, parfaitement complémentaire, m'auront permis d'aller jusqu'au bout, et de surmonter les phases de doutes que j'ai pu rencontrer.

Je remercie également l'ensemble des membres de l'ISCJ, et tout particulièrement les Professeurs Valérie MALABAT, Aurélie BERGEAUD, Évelyne BONIS, ainsi que le Doyen Jean-Christophe SAINT-PAU. Alors que j'ai réalisé l'essentiel de cette étude à distance, c'est un accueil chaleureux et agréable qui m'a toujours été réservé lors de mes venues à Bordeaux.

Dans ce contexte d'éloignement géographique, Tiphaine DOURGES, Doctorante en droit privé et sciences criminelles à l'ISCJ, m'a régulièrement aidé, et sa présence a constitué un lien fort avec l'ISCJ.

Je souhaite aussi exprimer ma reconnaissance à Adrien DEFOSSEZ, Maître de conférences en sociologie, qui m'a obligé à prendre de la hauteur et du recul avec mon sujet.

Je remercie enfin tous mes proches dont, notamment, Rita HABIB, Docteur en informatique, pour son amitié, son soutien moral et, surtout, pour son aide dans les traductions en anglais, ainsi que Ghazar CHAHBANDARIAN, également Docteur en informatique, qui est venu à mon secours chaque fois que mes connaissances techniques n'étaient plus suffisantes. Je n'oublie pas Abdo MALAC, Docteur en informatique et Ingénieur de Recherche, sans qui je n'aurais pas intégré l'enseignement supérieur et la recherche et qui, alors que les présents travaux n'étaient qu'un projet voire un simple désir, m'a convaincu de l'intérêt d'une telle démarche.

SOMMAIRE

(Un plan détaillé figure à la fin de la thèse)

ABREVIATIONS ET SIGLES UTILISES

Al.	Alinéa
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
Art.	Article
Ass. plén.	Assemblée plénière de la Cour de cassation
CA	Cour d'appel
CAA	Cour administrative d'appel
C. civ.	Code civil
Circ.	Circulaire
CEDH	Cour Européenne des Droits de l'Homme
CNIL	Commission Nationale de l'Informatique et des Libertés
Cons. const.	Conseil constitutionnel
C. pén.	Code pénal
C. pr. civ.	Code de procédure civile
C. pr. pén.	Code de procédure pénale
Crim.	Chambre criminelle de la Cour de cassation
C. séc. int.	Code de la sécurité intérieure
JLD	Juges des libertés et de la détention
PNIJ	Plateforme Nationale des Interceptions Judiciaires
Resp.	Respectivement
RGPD	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)
s.	Suivant
STAD	Système de Traitement Automatisé de Données
TGI	Tribunal de Grande Instance
T. conf.	Tribunal des conflits

INTRODUCTION

1. La donnée informatique au centre des investigations numériques. – Lorsqu'une enquête est ouverte au sein d'une procédure pénale, la finalité des investigations est de verser des éléments au dossier, destinés à la faire progresser. *In fine*, ces éléments font partie intégrante de l'ensemble des pièces permettant de clore celle-ci[3]. Au sein de ces investigations, les investigations numériques ont pour particularité de rechercher, d'exploiter, de manipuler et de générer des données.

2. Cette donnée informatique constitue la caractéristique commune des investigations numériques. Elle contribue, tout à la fois, à les définir et à leur conférer des spécificités, de sorte que l'étude des investigations numériques repose et s'articule autour de la donnée informatique.

3. Un contexte global de numérisation de notre société. – Les données informatiques sont le support de la vague de numérisation que connait actuellement notre société. Les conséquences de cette numérisation généralisée des informations touchent tous les domaines, dont le droit, notamment au travers de la recherche des preuves.

4. Des obstacles à la numérisation des investigations. – Le plus souvent, les conséquences de la numérisation dans un domaine professionnel sont la mise en place d'outils numériques dont l'objectif est l'amélioration de la qualité, de l'efficacité et de la performance.

Toutefois, en procédure pénale, le déploiement de certains de ces outils, qui pourraient améliorer à la fois l'efficacité des investigations et la qualité des données enregistrées dans les traitements de données judiciaires, se heurte à diverses difficultés.

5. Les effets négatifs de la non-intégration de certaines technologies informatiques à l'enquête. – En premier lieu, le prérequis est de définir la notion de donnée informatique et les termes qui en découlent directement.

---

[3] La clôture d'un dossier ne se solde pas systématiquement par un jugement. Il peut s'agir d'un classement sans suite, d'une ordonnance de non-lieu, de la découverte d'une personne dont la disparition était inquiétante, etc.
ROUSSEL Gildas, *Procédure pénale*, 8ème édition, Vuibert, p1 : « […] la procédure pénale […] correspond aux règles de forme et de procédure, régissant la recherche de la vérité (enquêtes, instructions) […] ».

La numérisation de notre société, dont la donnée informatique est le support, a des conséquences sur la dématérialisation des investigations au sein de l'enquête. Cet effet doit, en deuxième lieu, être étudié pour analyser comment les investigations diligentées dans le cadre d'une procédure pénale se sont actuellement adaptées à cette numérisation. En troisième lieu, un constat se dégage alors : toutes les nouvelles techniques informatiques issues de la numérisation n'ont pas encore pénétré les investigations. Les bénéfices potentiellement importants que pourraient apporter ces nouveautés technologiques aux investigations constituent un enjeu majeur pour l'évolution de la procédure pénale.

En conséquence, il est nécessaire de préciser ce qu'est une donnée informatique *(§1)* pour pouvoir étudier comment la numérisation de notre société a pénétré les investigations au sein de l'enquête *(§2)*. Néanmoins, certaines techniques ne sont pas encore exploitées par les investigations, ce qui constitue un frein à l'amélioration potentielle de l'enquête pénale *(§3)*.

§1. La notion de donnée informatique

6. La donnée comme support numérique d'une information. – Le mot « donnée » comporte plusieurs sens[4]. Dans la suite de la présente étude, dans un objectif de lisibilité, « donnée » sera utilisé au sens de « donnée informatique ».

Dans cette acception, l'emploi du mot « donnée » dans le vocabulaire courant est devenu banal, du moins dans les sociétés technologiquement avancées. Lorsque ce mot est entendu ou prononcé, plus personne ne s'interroge sur sa capacité à le définir.

7. La donnée est le support numérique d'une information[5]. Elle est donc définie par son objet qui est, tout d'abord, de donner une existence numérique à une information puis, ensuite, de la conserver, comme le ferait le papier.

8. Une notion évidente dans les sciences informatiques. – Les scientifiques en informatique n'éprouvent pas le besoin de définir la donnée qui, pour eux, est également l'entité qui permet le stockage numérique de l'information. Cependant, les informaticiens emploient rarement ce mot au singulier, lui préférant systématiquement le pluriel.

[4] Les données d'un problème en mathématiques, ce qui sert de base, l'idée fondamentale d'une œuvre, etc. Source : Centre National de Ressources Textuelles et Lexicales.

[5] Dictionnaire Larousse : « Représentation conventionnelle d'une information en vue de son traitement informatique. » Source : www.larousse.fr

Celui-ci illustre qu'une information nécessite le plus souvent plusieurs données pour être stockée dans un support numérique comme un disque dur ou une clé USB.

9. La corrélation entre les données et l'information. – Pour que ces données stockées dans un support numérique prennent du sens et révèlent l'information qu'elles représentent, les informaticiens expliquent qu'un dispositif d'interprétation est nécessaire[6]. Ils opèrent donc une distinction entre la donnée lue, par exemple, par l'utilisateur d'un ordinateur qui voit une information intelligible sur son écran, et la donnée brute (appelée en informatique *Raw Data*[7]*)*. Cette dernière est codée sous forme de signaux électriques ou magnétiques écrits sur le support, en amont de toute interprétation par le dispositif prévu à cet effet.

10. Une difficulté pour reconstruire l'information. – Dans des situations très rares et très particulières, l'interprétation des données pour donner un sens à des informations est délicate et incertaine.

C'est notamment le cas lorsque le dispositif d'interprétation des données casse. Par exemple, lorsque la partie électronique du disque dur est détériorée, l'opération qui va consister à récupérer les informations à partir des données brutes qui sont écrites sur le disque est compliquée. Pour preuve, des sociétés spécialisées proposent ce type de prestations[8].

La récupération des informations à partir des données brutes n'est pas toujours possible, et il n'est pas rare qu'elle ne soit que partielle. En conséquence, il existe, dans ce cas, une différence résiduelle entre les données brutes stockées sur un support numérique et les informations qui ont été précédemment enregistrées sur celui-ci par un utilisateur.

11. Une différence résiduelle sans conséquence. – Cette différence entre « information » et « donnée » pourrait, au premier abord, susciter un vif émoi chez les juges qui ont régulièrement, dans les dossiers dont ils sont saisis, des décisions à prendre à partir d'informations extraites d'une source numérique.

Cette situation reste toutefois rare et circonscrite à des situations très particulières.

---

[6] Il peut s'agir d'une couche logicielle, ou du contrôleur d'un disque dur ou d'une clé USB, etc.

[7] www.wikipedia.org : « Raw data, also known as primary data, is data […] collected from a source. […] As well, raw data has not been subject to any other manipulation by a software program or a human researcher, analyst or technician. […] The term "raw data" can refer to the binary data on electronic storage devices, such as hard disk drives (also referred to as "low-level data"). »

[8] V. par ex. Kroll Ontrack, Recoveo, etc.

12. Lorsque le juge se pose une question d'ordre technique telle que, par exemple, un doute sur les informations qui seraient issues d'une récupération d'un disque dur cassé, un expert est saisi[9]. Dans ce cas, bien évidemment, la fiabilité de la chaîne judiciaire repose sur la clarté que vont avoir les experts à décrire dans leur rapport le degré de certitude de l'information qu'ils énoncent, afin que les magistrats en aient connaissance et puissent appréhender la véracité de l'interprétation[10].
On peut, sur ce point, faire le parallèle avec les comparaisons ADN où les biologistes indiquent systématiquement un pourcentage de concordance[11].

13. L'évidence de la définition de la « donnée » dans la doctrine juridique. – Hormis des situations marginales qui supposeraient systématiquement l'intervention d'experts dans une procédure judiciaire pour débattre de la fiabilité des informations obtenues à partir de certaines données, la corrélation entre la donnée et l'information qu'elle stocke est considérée, par tous, comme une évidence.
14. C'est le cas dans la doctrine juridique[12]. Les auteurs considèrent comme un acquis la compréhension de ce qu'est une donnée informatique, se consacrant à définir des typologies de données particulières : « données à caractère personnel[13] » ou, plus récemment, « données ouvertes[14] » ou « *big data*[15] ».

---

[9] V. *infra* n°300.
[10] LEMOINE Vincent, *Le régime juridique des constatations policières sur internet,* L'Harmattan. Avec la vision technique qui est la sienne, Vincent LEMOINE confirme que « l'expert ou le procès-verbal rédigé par l'enquêteur doit décrire le plus précisément possible la méthode utilisée ».
[11] MOUSTIERS Anaïs, *Preuve et biotechnologies : l'utilisation des empreintes génétiques à des fins judiciaires,* La preuve pénale sous la direction d'Olivier de FROUVILLE, La documentation Française, p. 194 : « Les preuves scientifiques fournissent une probabilité de la réalité d'un fait ou d'un acte. Or, si la probabilité est grande, voire quasi absolue, la preuve désignée sera assimilée à une certitude. »
[12] CORNU Gérard, *Vocabulaire juridique,* 10ème édition, puf : seules des catégories de données sont définies, à savoir les « données à caractère personnel » et les « données sensibles ».
Données à caractère personnel : « toute information relative à une personne physique permettant son identification directement […] ou indirectement […]. »
[13] *Ibid.* V. également PERRAY Romain, *Données à caractère personnel – Introduction générale et champ d'application de la loi "Informatique et libertés*, JurisClasseur Communication Fasc 930 : « Dans cette logique, les actuelles dispositions de la loi « Informatique et libertés » ont remplacé l'ancienne notion d'"informations nominatives" par une définition – plus neutre et plus large – de "données à caractère personnel", incluant notamment la voix et l'image, et qui a vocation à s'appliquer à toute information, dès lors qu'elle permet d'identifier nominativement une personne physique ou même seulement de la rendre identifiable, voire simplement de la singulariser »
[14] A noter que le terme anglo-saxon *open data* est beaucoup plus utilisé. www.opendefinition.org (Open Knowledge Foundation) - « Une donnée n'est ouverte que s'il est possible de l'utiliser, de la réutiliser et de la redistribuer librement – avec, comme seules conditions admissibles, d'une part, l'obligation d'en mentionner la source et, d'autre part, la nécessité de permettre la réutilisation de toute base de donnée dérivée sous les mêmes conditions que la base de donnée originale (share-alike). »
[15] BOURCIER Danièle et DE FILIPPI Primavera, *L'Open Data : universalité du principe et diversité des expériences ?*, Semaine Juridique Administrations et Collectivités territoriales, n° 38, Septembre 2013 :

Il en est de même avec la CNIL[16] qui adopte une position similaire à la doctrine juridique. Elle ne juge pas utile de définir la donnée « seule », et s'intéresse directement à des données particulières telles que la « donnée personnelle[17] » et la « donnée sensible[18] ».

15. La donnée comme support de la dématérialisation. – Le point en commun de toutes les données, quelle que soit la catégorie dans laquelle elles sont classées par la doctrine juridique ou les autorités publiques, est de donner une existence numérique à une information qui, par voie de conséquence, est alors dématérialisée.

16. La dématérialisation comme support de la numérisation de notre société. – L'expression « numérisation de notre société » se réfère au fait que la vie des individus qui la composent, ainsi que l'ensemble de leur environnement, reposent de plus en plus sur des informations numériques.

La dématérialisation des informations fait partie de la numérisation de notre société puisqu'elle se définit comme l'action de rendre les informations immatérielles[19]. La dématérialisation s'oppose aux documents reprographiés et elle est souvent associée aux démarches « zéro papier[20] » qui tendent actuellement à se généraliser dans le grand public[21].

« La plupart des données que nous rencontrons sur le réseau ont été constituées au fur et à mesure. Soit elles sont restées isolées en petits ensembles de données, soit elles ont été agrégées à partir de sources différentes, pour être ensuite regroupées en des ensembles structurés qui peuvent parfois faire l'objet de grandes bases de données (Big Data). »

[16] Commission Nationale de l'Informatique et des Libertés, définie aux articles 8 et s. de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

[17] www.cnil.fr : « Toute information identifiant directement ou indirectement une personne physique (ex. nom, n° d'immatriculation, n° de téléphone, photographie, date de naissance, commune de résidence, empreinte digitale...). »

[18] *Ibid*. : « Information concernant l'origine raciale ou ethnique, les opinions politiques, philosophiques ou religieuses, l'appartenance syndicale, la santé ou la vie sexuelle. En principe, les données sensibles ne peuvent être recueillies et exploitées qu'avec le consentement explicite des personnes. »

[19] V. *infra* n°219.

[20] Ces démarches sont courantes au sein des entreprises ou des administrations pour réduire, non seulement le coût direct du papier, mais également les coûts d'archivage induits par leur volume. Elles consistent à gérer l'ensemble des informations, des circuits de validation de documents (par exemple, des devis, des demandes de congés, etc) directement dans le système d'information.

[21] Les fournisseurs d'énergie, de téléphonie, etc, proposent systématiquement d'envoyer les factures sous forme numérique. L'argument invoqué est la réduction du coût environnemental.

§2. Les conséquences de la numérisation de notre société

17. Des bouleversements dans les échanges d'informations. – La numérisation de notre société pousse tous les domaines à intégrer des modifications dans la façon de communiquer et de travailler. Ces changements sont dus à l'arrivée de nouveaux outils issus de la dématérialisation des informations et des échanges, qui n'ont désormais d'existence qu'au travers de données.

Certains effets généraux de la numérisation de notre société doivent être observés *(I)* car ils permettent de mieux comprendre les conséquences de cette numérisation sur le droit *(II)*.

I – Les effets généraux de la numérisation de notre société

18. La technique guidée par les usages. – Le point de départ de la numérisation de notre société repose sur les progrès informatiques et électroniques[22]. L'appropriation de ces techniques par les sociétés modernes dans un contexte global de dématérialisation de la vie quotidienne, dépasse désormais largement les disciplines informatiques et électroniques. Ces dernières se retrouvent positionnées en tant que support aux utilisations qu'elles permettent, créant ainsi une sorte d'innovation inversée : ce ne sont plus des progrès technologiques qui induisent des nouvelles utilisations, mais des besoins sociétaux qui appellent des évolutions techniques.

19. L'influence structurante de la numérisation sur notre société. – Les sociologues analysent la numérisation de notre société au travers de ses effets sur les réseaux sociaux[23] ou sur une structure sociale[24].

---

[22] Dans le domaine de la numérisation, et notamment pour la téléphonie mobile ou les objets connectés, les progrès informatiques (en réseau, en systèmes embarqués, en système d'exploitation, etc) sont inextricablement associés à des avancées technologiques en électronique (amélioration des débits de communication, miniaturisation, etc).

[23] L'expression « réseaux sociaux » ne doit pas être entendue au sens « Facebook », « Instagram », ou autres, mais au sens sociologique, c'est-à-dire de « relations sociales » (v. *infra* Michel GROSSETTI).

[24] C'est-à-dire sur une population déterminée d'individus soumise à un contexte précis.
DEFOSSEZ Adrien, *Soutien social et réseau personnel au cœur de l'expérience du cancer,* thèse soutenue le 9 décembre 2014, Université de Toulouse : il est notamment étudié l'impact de la numérisation de notre société sur les personnes atteintes du cancer.
GROSSETTI Michel, *Que font les réseaux sociaux aux réseaux sociaux ? Réseaux personnels et nouveaux moyens de communication,* Réseaux n°184-185, 2014/2-3 p.187 : Michel GROSSETTI interprète les données de plusieurs études pour montrer que les spécificités de l'impact sur la communauté homosexuelle des réseaux de rencontre en ligne. Ces réseaux de rencontre en ligne sont évidemment le fruit et l'une des illustrations de la numérisation de notre société.

Même si certains, comme Michel GROSSETTI, pensent que les nouvelles technologies de la communication ne révolutionnent pas ces relations sociales et ne font qu'accompagner les évolutions que notre société connait depuis la fin de la deuxième guerre mondiale[25], tous s'accordent à reconnaître l'influence structurante que la numérisation a sur notre société[26].

20. L'impact sur la vie quotidienne et le comportement individuel de tout un chacun est alors très important[27] puisque, même si les relations sociales ne sont pas révolutionnées d'un point de vue sociologique, les vecteurs de communication ont changés en faisant des échanges numériques un support central dans les relations entre les individus.

21. L'influence de la numérisation sur les activités professionnelles. – Ces nouveaux supports et moyens de communication sont aussi bien utilisés au sein des réseaux sociaux relevant de la sphère privée, que professionnelle. Les entreprises ou les administrations entendent profiter de l'accélération des échanges[28] que ces outils apportent, dans un objectif d'amélioration de la productivité, de la qualité et de la performance de leurs salariés ou de leurs agents.

22. Cette influence de la numérisation sur les activités professionnelles est déterminante pour la présente étude puisqu'elle va avoir d'importantes conséquences sur les matières juridiques. Ce sont, à la fois, les règles de droit substantiel et le droit processuel, qui prennent de plus en plus en compte, non sans difficulté, les données comme support incontournable des informations et des échanges.

---

[25] *Ibid.*

[26] DENOUËL Julie et GRANJON Fabien, *Communiquer à l'ère numérique,* Edition Mines ParisTech, 2011, p. 8 : « La « culture numérique » en émergence structure l'évolution de la société et les NTIC se présentent toujours davantage comme un passage obligé pour accomplir de plus en plus de tâches du quotidien. »

[27] *Ibid.* « […] les usages des dispositifs numériques sont devenus des activités parmi les plus ordinaires dans la mesure où elles s'intègrent toujours davantage au quotidien des individus et se présentent parfois même comme des impératifs pratiques. »

[28] V. par ex. GROSSETTI Michel, *ibid.* : « Le principal changement apporté par l'existence des moyens électroniques de communication semble bien concerner la temporalité des échanges. En simplifiant, on pourrait dire que le numérique ne dilate pas tant l'espace qu'il accélère le temps. »

II – Les effets de la numérisation de notre société sur le droit

23. La culture de l'écrit remise en question. – Historiquement et traditionnellement, le droit repose sur l'écrit[29]. Dans l'ancien testament, lorsque Dieu choisit Moïse pour édicter les dix commandements, il ne se contente pas de les lui énoncer verbalement. Il assortit ses paroles des Tables de la Loi, qu'il remet à Moïse pour figer sur la pierre, et donc par écrit, les règles considérées comme essentielles par de nombreuses religions.
Au travers de cet exemple, forçant volontairement le trait, il est possible de mesurer l'ampleur de la remise en question, pour le droit, que représente la dématérialisation des informations et des échanges. Désormais, l'écrit n'est plus le seul vecteur incontesté de circulation et de transmission des informations. Il doit partager cette prérogative avec les données informatiques.

24. Cette remise en question a, bien sûr, des effets sur le droit en général *(A)* et, plus particulièrement, sur la matière pénale *(B)*.

A. Les effets généraux sur le droit

25. Une adaptation du droit interne aux nouvelles technologies. – La prise en compte de la numérisation de notre société par le droit n'est pas isolée et unique. Elle se rapproche de l'adaptation à d'autres évolutions technologiques[30], telles que, par exemple, l'intégration du résultat des analyses génétiques en tant qu'élément de preuve[31].

26. Une adaptation transversale et générale. – Pour autant, les adaptations du droit pour prendre en compte la numérisation de notre société sont différentes de l'intégration des autres technologies. En aucun cas, il ne s'agit d'établir une sorte de hiérarchie sur l'importance que revêtent des technologies radicalement différentes au sein des dossiers judiciaires, mais de constater que la dématérialisation des informations a des

[29] Les historiens du droit commencent à parler de « rédaction écrite des coutumes » (CASTALDO André et MAUSIN Yves, *Introduction historique au droit,* 4ème édition, Dalloz, p.132) et de « codification des usages » (DEVAUX Olivier, *Histoire des institutions de la France (1er – XIVème siècle)*, L'Hermès, p.51) dès le moyen âge.
[30] DEMARCHI Jean-Raphaël, *Les preuves scientifiques et le procès pénal*, LGDJ, 2012. Thèse soutenue en 2010 à Nice.
[31] V. par ex. en droit civil, la filiation qui a été profondément transformée. Auparavant, il n'était pas rare qu'une paternité soit juridiquement prononcée sans aucune réalité biologique. Depuis l'arrivée des analyses génétiques, la force probatoire de cette technique s'est imposée et la réalité technique dicte la décision judiciaire en matière de filiation.
HAUSER Jean, *Filiation – Identification génétique. – Procréation médicalement assistée*, JurisClasseur Code civil : « Alors que le droit antérieur privilégiait la vision utilitaire de la filiation, fût-ce au prix de contre-vérités biologiques, la loi nouvelle renonçait pour une large partie à cette vision. La primauté était donc donnée à la vérité biologique […]. »

conséquences beaucoup plus transversales sur les procédures[32], ainsi que sur le droit substantiel interne.

27. Une adaptation du droit interne ancienne. – La première adaptation majeure de notre droit positif à la numérisation des informations remonte à 1978 avec la loi informatique et libertés[33]. Son seul titre, au travers du mot « informatique », démontre que les autorités publiques avaient perçu, dès la fin des années soixante-dix, les conséquences majeures que la donnée allait avoir sur la collecte des informations personnelles.

28. Une adaptation du droit interne continue. – Depuis 1978, l'adaptation est continue avec des modifications plus ou moins importantes. Récemment, la réforme de 2016 du droit des obligations dans le Code civil est, notamment, venue consacrer le contrat conclu par voie électronique[34]. Ce faisant, le droit civil se pose en modèle d'adaptation à la dématérialisation des échanges.

29. L'origine internationale de certaines adaptations. – Néanmoins, cette adaptation « modèle » est en fait imposée par l'aspect transfrontalier des échanges numériques qui facilite et banalise désormais le commerce international à distance. Notre droit interne a donc dû réagir sous cette influence externe pour, par exemple, mieux protéger les consommateurs français, en encadrant les contrats conclus par voie électronique[35].

30. Dans un autre domaine qu'est celui de la protection des données à caractère personnel, l'influence de l'Europe est majeure depuis 1995. La directive du 24 octobre 1995[36] avait fixé un cadre commun. Celle-ci vient d'être remplacée par le règlement

[32] V. *infra* n°46.
[33] Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.
[34] Ordonnance n°2016-131 du 10 février 2016 portant réforme du droit des contrats, du régime général et de la preuve des obligations. Ce texte a introduit, notamment, les articles 1125 et s. (sous-section 4 de la section 1 relative à la conclusion du contrat) et 1174 et s. (sous-section 2 de la section 3 relative à la forme du contrat) dans le C. civ. Ces deux séries de dispositions sont propres aux contrats conclus par voie électronique.
[35] *Ibid.* Plusieurs articles introduisent des dispositions plus protectrices pour les non-professionnels (v. par ex. C. civ. 1127, 1127-3).
[36] Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

général sur la protection des données[37] (ci-après RGPD), entré en application le 25 mai 2018. L'application directe dans les états membres, dont la France, de la majorité des mesures, démontre cette influence externe sur notre cadre légal.

B. Les effets sur la matière pénale

31. Une influence internationale plus focalisée. – En matière pénale, l'influence du contexte international de la numérisation de notre société sur l'adaptation de notre droit interne est différente. En droit civil, des pans entiers découlent directement de l'influence européenne, comme le droit des obligations[38] ou la protection des données personnelles. Certes, en matière pénale, des règles ont également une origine purement européenne : le mandat d'arrêt européen[39] ou la décision d'enquête européenne[40]. Pour autant, l'influence de la numérisation de notre société par des décisions prises au niveau d'instances internationales sur le droit pénal ou la procédure répressive est plus ciblée qu'en droit civil.

Dans ce contexte, il convient de distinguer les conséquences de la numérisation de notre société sur le droit pénal substantiel *(1)* et sur la procédure pénale *(2)*.

1. Les effets sur le droit pénal substantiel

32. Les effets transfrontaliers des échanges numériques. – La cybercriminalité[41] est apparue dans le contexte numérique de la mondialisation. La notion de frontière n'a que peu de sens lorsqu'il est question d'échanges sur Internet. Ainsi, la nouvelle forme de criminalité qui consiste à attaquer des plateformes informatiques accessibles au travers d'Internet, se trouve facilité par cette mondialisation. Une première difficulté majeure se pose alors, pour que le droit pénal substantiel national puisse réprimer efficacement ces comportements transfrontaliers.

[37] 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).
[38] PORCHY-SIMON Stéphanie, *Droit Civil – Les obligations,* Dalloz, 9ème édition. L'auteure parle de la forte « influence du droit communautaire » et évoque le projet de « création d'un réel droit européen des contrats. »
[39] C. pr. pén art. 695-11 et s.
[40] C. pr. pén. art. 694-15 et s.
[41] Pour une étude sur la définition de la cybercriminalité, v. CABON Sarah-Marie, *Atteintes aux systèmes de traitement automatisé de données – L'influence du cyber espace sur la criminalité économique et financière,* LexisNexis, Droit pénal n°3, mars 2018, étude 5.

33. C'est pourquoi la cybercriminalité est une source de réflexion importante dans la doctrine juridique. Elle fait l'objet de nombreuses études et publications depuis presque dix ans[42]. Ces travaux mettent en exergue la complexité du problème que rencontrent tous les états dits développés, pour protéger efficacement leurs infrastructures[43] et les acteurs économiques du pays, qui ne doivent pas souffrir d'attaques susceptibles de les affaiblir. La complexité tient dans l'impossibilité de pouvoir créer, unilatéralement, des infractions permettant de punir cette nouvelle forme de criminalité qui utilise les frontières étatiques pour commettre des agissements délictueux sur Internet en toute impunité.

34. L'adaptation des infractions aux attaques au travers d'Internet. – Pour qu'un état puisse se protéger contre ces cyberattaques, les agissements numériques répréhensibles doivent pouvoir faire l'objet de poursuites. C'est l'objectif des infractions réprimant les « atteintes aux systèmes de traitement automatisé de données[44] » qui punissent un ensemble d'actions visant à nuire, à distance, à un système informatique. La répression de ces agissements néfastes est générale, dans le sens où elle s'intéresse indistinctement à des actes qui peuvent être commis, aussi bien depuis un pays étranger, que depuis un ordinateur situé à proximité, comme au sein d'une entreprise.

35. L'adaptation des infractions aux mauvaises utilisations d'Internet. – L'aspect transfrontalier des échanges numériques impose une autre forme d'adaptation du droit pénal spécial interne. Il faut pouvoir punir les conséquences d'une sorte de délinquance passive sur Internet. En effet, la cybercriminalité qui vient d'être vue consiste, pour des délinquants, à attaquer au travers d'actions « actives » des systèmes informatiques distants. A l'inverse, lorsque des individus mettent en ligne sur Internet des contenus répréhensibles accessibles à tous, tels que de la pédopornographie ou faisant l'apologie du terrorisme, ces personnes ne procèdent plus à aucune action une fois que les pages *Web* sont en lignes.

36. Certes, les autorités publiques répriment la diffusion de tels contenus[45], mais l'aspect transfrontalier de la diffusion de contenu ne laisse que peu d'espoir pour les

[42] V. les nombreux articles de QUEMENER Myriam, CAPRIOLI Eric ou FERAL-SCHUHL Christiane sur ce sujet.
[43] C'est dans cet objectif qu'ont été créés, dès 2006, les opérateurs d'importance vitale (dits OIV). V. décret n°2006-212 du 23 février 2006 relatif à la sécurité des activités d'importance vitale codifié en 2007 par le décret n°2007-585 du 23 avril 2007 relatif à certaines dispositions réglementaires de la première partie du code de la défense) dans le Code de la défense (art. R.1332-3 et s.).
[44] C. pén. art.323-1 et s.
[45] Pour la pédopornographie : C. pén. art. 227-23. Pour la diffusion de contenus faisant l'apologie du terrorisme : C. pén. art. 421-2-5 et 421-2-5-1.

autorités publiques françaises de pouvoir punir les auteurs de tels contenus. Le droit pénal spécial s'est donc adapté en punissant la consultation de ces sites qui, pour sa part, est commise sur le territoire national. C'est notamment le cas en matière de pédopornographie[46].

37. Les difficultés des infractions relatives à la consultation. – Dans le cas de la consultation de sites faisant l'apologie du terrorisme[47], la création d'infractions à cette fin soulève plus de difficultés, comme en témoignent l'ancien article 421-2-5-2 du Code pénal qui, par deux fois, a fait l'objet d'une déclaration d'inconstitutionnalité[48], ainsi que l'article 421-2-5 dont la portée a été encadrée par le Conseil Constitutionnel[49].
En premier lieu, l'ancien article 421-2-5-2 avait pour objectif de réprimer la consultation de sites faisant l'apologie du terrorisme. En second lieu, l'article 421-2-5 punit la provocation à commettre et l'apologie des actes de terrorisme.
Dans les deux cas, l'intention du législateur est de punir le plus en amont possible de la commission d'un acte terroriste, des personnes susceptibles de passer à l'acte.

38. Les difficultés de l'adaptation à la numérisation de notre société. – Les difficultés dont il vient d'être question, que rencontrent les autorités publiques pour punir certaines consultations de sites Internet, aux origines internationales, ne sont qu'une illustration des problèmes que posent l'adaptation du droit pénal spécial interne à la numérisation de notre société.

39. En effet, d'autres problèmes, purement nationaux, tels que le vol de données, en sont un autre signe. Pendant de nombreuses années, seul le vol simple[50] existait, alors que les données étaient d'ores et déjà un support d'information largement répandu. Ainsi, lorsque des informations étaient dérobées sous forme de données, il n'existait pas d'autre solution que de qualifier les faits délictueux avec l'infraction de vol simple. Or, l'aspect immatériel des données[51] faisait naître une ambiguïté importante avec la notion de

[46] C. pén. art. 227-23 4ème al.
[47] Sur la notion d'apologie, v. crim, 4 juin 2019 n°18-85.042 – LEPAGE Agathe, *Contribution à l'interprétation de la notion d'apologie*, LexisNexis Communication Commerce Electronique n°9, sept. 2010, comm. 55.
[48] Dans sa première version (Cons. const. : décision n°2016-611 QPC du 10 février 2017) puis dans sa deuxième (Cons. const : décision n°2017-682 QPC du 15 décembre 2017).
[49] Crim. 24 mars 2020 n°19-86.706 : JurisData n°2020-004614.
Cons. Const. : décision n°2020-845 QPC du 19 juin 2020.
[50] C. pén. art. 311-1.
[51] V. *infra* n°219.

« soustraction frauduleuse de la chose d'autrui » qui se réfère implicitement à un bien matériel[52]. L'arrêt « Bourquin[53] » incarne cette ambiguïté en faisant référence au vol « du contenu informationnel » enregistré dans des disquettes. Néanmoins, l'ambiguïté est nuancée car le vol est bien caractérisé car il y avait, préalablement, le vol « physique » des disquettes au sein desquelles étaient présentes les informations numériques.

40. Il aura fallu attendre 2014, pour qu'une loi[54] vienne modifier l'article 323-3 du Code pénal, tentant ainsi de lever ces ambiguïtés[55]. Ces dernières perdurent dans la jurisprudence de la chambre criminelle de la Cour de cassation, car celle-ci continue, marlgré la modification de l'article 323-3, à appliquer l'infraction de vol à la soustraction frauduleuse de données[56]. Au demeurant, il est intéressant de noter que le législateur a choisi de punir plus lourdement ce vol de données informatiques[57] que le vol simple[58], ce qui illustre la prise en compte par les autorités publiques, de l'importance de protéger les données au sein de la société actuelle.

41. Les nombreux effets de la numérisation sur le droit pénal. – Comme précédemment évoqué, les effets de la numérisation de notre société sur le droit en général sont fortement transversaux[59]. Il en est de même avec le droit pénal substantiel. En effet, plusieurs livres du Code pénal sont concernés par la création d'infractions découlant de cette numérisation[60]. De plus, l'adaptation des infractions à l'environnement numérique génère souvent des difficultés, comme pour la consultation des sites faisant l'apologie du terrorisme ou, de manière plus prégnante encore, pour prendre en compte le vol des données.

---

[52] JACOPIN Sylvain, *Le début d'une évolution sur la nature de la chose susceptible d'appropriation frauduleuse,* LexisNexis Droit pénal n°4, avril 2001, chron. 16 : sur l'application de l'article 311-1 du C. pén. et la matérialité des choses soustraites frauduleusement.
Crim. 20 mai 2015 n°14-81336. CONTE Philippe, *Vol d'information,* LexisNexis, Droit pénal n°10, Octobre 2015, comm. 123.

[53] Crim. 12 janv. 1989 : Bull. crim. n° 14 ; Gaz. Pal. 1989, 2, somm. p. 283 ; Rev. sc. crim. 1990, p. 346, note P. Bouzat.

[54] Loi n°2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme.

[55] DETRAZ Stéphane, *Vol de données informatiques,* Gazette du palais, 18 juin 2015 n°169, p.8.

[56] Crim. 28 juin 2017 n°16-81.113 : JurisData n°2017-012975. CONTE Philippe, *Vol - Soustraction d'une information*, LexisNexis Droit pénal n°10, Octobre 2017, comm. 141.

[57] 5 ans d'emprisonnement et 150 000 € d'amende.

[58] 3 ans d'emprisonnement et 45 000 € d'amende.

[59] V. *supra* n°26.

[60] Les infractions aux données personnelles sont dans le Livre II (art. 226-16 et s.), celles relatives aux systèmes de traitement automatisé de données dans le Livre III et la consultation de sites faisant l'apologie du terrorisme sont dans le Livre IV.

2. Les effets sur la procédure pénale

42. Deux conséquences différentes. – La numérisation de notre société impose une rupture idéologique au droit en remettant en question la culture de l'écrit[61]. Au sein de la matière pénale, cet effet est tout particulièrement vrai en procédure où le besoin de dématérialiser les informations et les échanges apparaît comme une nécessité[62], notamment pour répondre aux besoins internationaux. Par ailleurs, une similitude existe avec le droit pénal spécial. En effet, la numérisation a induit la création d'infractions sanctionnant des actions visant, soit à nuire à des données, soit à utiliser des données pour commettre des actes répréhensibles. Sur un schéma analogue, la procédure pénale s'est adaptée en créant des actes d'investigations permettant d'enquêter sur des données ou grâce à des données.

Il convient donc de distinguer les conséquences de la numérisation sur la dématérialisation des informations au sein de la procédure *(a)*, des effets qui ont conduit à créer des actes d'investigations dédiés aux données *(b)*.

a. La dématérialisation du support administratif des procédures pénales

43. Des échanges nationaux et internationaux. – La dématérialisation des informations et des échanges poursuit invariablement deux objectifs. Le premier est de pouvoir stocker une plus grande masse d'informations, facilement exploitables. Le second est de pouvoir échanger plus rapidement ces informations stockées.

Ces deux aspects de la dématérialisation répondent à des besoins, à la fois au niveau international et au niveau national.

44. L'optimisation des échanges internationaux d'informations. – L'internationalisation de la grande délinquance[63] et le terrorisme nécessitent que des fichiers transfrontaliers soient créés. Au-delà du signalement d'individus dangereux[64], ils ont également vocation de permettre le suivi des déplacements des personnes, notamment

[61] V. *supra* n°23.

[62] BOULAKRAS Haffide, *La procédure pénale numérique (PPN) : promesses, apports et réalisations*, LexisNexis, Droit pénal n°3, mars 2020

[63] SOURISSEAU Yann, *La poursuite des réseaux de prostitution*, Dalloz AJ Pénal 2012 p.201.
Les réseaux de prostitution s'inscrivent dans la traite des êtres humains et sont organisés sur plusieurs pays avec des « recrutements » dans des pays où la misère est fortement présente et une prostitution qui s'organise dans des pays comme la France.
Il en est de même avec le trafic de drogue qui est structuré sur plusieurs pays, notamment pour assurer l'approvisionnement.

[64] Système d'Information Schengen : v. *infra* n°705.

par voie aérienne[65]. Ces données peuvent également servir pour établir des rapprochements entre différents individus qui auraient voyagés ensemble.

45. En Europe, les enquêtes pénales bénéficient de cette vitesse dans les échanges apportés par la dématérialisation, puisque certaines mesures autorisent désormais que les demandes d'informations entre des autorités judiciaires de pays différents, puissent se faire par voie électronique[66]. Un degré supplémentaire émerge actuellement dans les échanges d'informations, en autorisant la mise en commun d'informations[67]. Il s'agit d'une coopération plus intégrée que les échanges ponctuels de données[68].

46. L'optimisation des échanges en procédure pénale interne. – Les pouvoirs publics ont débuté la dématérialisation des procédures civiles et administratives en 2005[69].

47. En procédure pénale, les démarches concrètes pour la numérisation de la procédure débutent véritablement avec la circulaire du 9 octobre 2006[70], puis se poursuivent avec le décret du 15 novembre 2007 qui fait avancer fortement cette dématérialisation[71]. Avant celui-ci, la reprographie était le seul moyen autorisé pour transmettre une copie d'un dossier. Le décret de 2007 offre la possibilité que la copie des actes du dossier d'instruction soit numérique[72], et que les fichiers correspondants puissent

[65] API-PNR : v. *infra* n°704.

[66] « Le système ECRIS (système informatisé d'échange d'informations sur les casiers judiciaires) a été créé en avril 2012 afin de faciliter l'échange d'informations sur les casiers judiciaires dans l'ensemble de l'UE. Il établit les interconnexions électroniques entre États membres et met en place des règles pour faire en sorte que les informations sur les condamnations figurant dans les systèmes de casier judiciaire des États membres puissent être échangées au moyen de formats électroniques standardisés, de manière uniforme et rapide, et dans des délais légaux de courte durée. » - Source : e-justice.europa.eu

[67] Conférence européenne de lutte contre le terrorisme, *Déclaration commune de sept ministres européens,* Paris, 5 novembre 2018 : « un registre judiciaire européen anti-terroriste placé auprès d'Eurojust sera alimenté par tous les Etats européens. Ce registre contiendra, notamment, l'identité des personnes condamnées ou des suspects dans les enquêtes en cours. »

[68] V. eg. l'ordonnance n°2016-1636 du 1er décembre 2016 relative à la décision d'enquête européenne en matière pénale.

[69] V. le 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, et notamment son art. 73.
V. pour la procédure administrative le décret n°2005-222 du 10 mars 2005 relatif à l'expérimentation de l'introduction et de la communication des requêtes et mémoires et de la notification des décisions par voie électronique.

[70] Circ. JUS A 0600-292C du 9 octobre 2006 : « plan de développement de la numérisation des procédures pénales. »

[71] Décret n°2007-1620 du 15 novembre 2007 modifiant le code de procédure pénale (troisième partie : Décrets) et relatif à l'utilisation des nouvelles technologies.
Sur l'avancé de la dématérialisation, v. CHEVALLIER Frédéric et BAILLARD Denys, *Le numérique au service du contradictoire,* LexisNexis, Droit pénal n°3, mars 2018, entretien 3.

[72] C. pr. pén. art. D15-7.

être envoyés aux avocats par voie électronique[73]. Ces fichiers sont au format *pdf* et contiennent la copie numérique de toutes les pièces cotées versées au dossier.

48. L'optimisation de l'archivage en procédure pénale interne. – La loi du 23 mars 2019[74] introduit un palier supplémentaire dans la dématérialisation du dossier de procédure[75]. Outre la numérisation des actes d'enquête ou d'instruction, c'est l'intégralité du dossier qui peut désormais être « conservé sous format numérique […], sans nécessité d'un support papier[76] ».

49. L'optimisation de l'ouverture d'une procédure pénale par une victime. – Depuis cette même loi de mars 2019, la possibilité est offerte à une victime de déposer plainte en ligne[77].

50. La modification de l'exercice du droit pénal. – La dématérialisation des échanges d'informations au sein d'une procédure pénale modifie l'exercice pratique du droit. En effet, la dématérialisation des procédures transforme les échanges entre les différents professionnels intervenants dans une procédure judiciaire[78]. Historiquement, les documents, pièces, conclusions, rapports d'expertise et autres correspondances étaient échangés sur support papier. Sur ce point, le fax, outil de prédilection des professions juridiques durant de nombreuses années, répondait à cette « culture du papier » puisque ce que recevait le correspondant était une missive imprimée. La dématérialisation de la procédure a précisément pour objectif de faire circuler l'information entre les différents professionnels intervenants dans un dossier pénal sous forme numérique, même si cette circulation de l'information reste insuffisante[79].

---

[73] C. pr. pén. art. D15-8.
[74] Loi n°2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice.
[75] V. eg. le décret n°2019-507 du 24 mai 2019 pris pour l'application des dispositions pénales de la loi n°2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice relatives à la procédure numérique, aux enquêtes et aux poursuites.
[76] C. pr. pén. art. 801-1, I.
[77] C. pr. pén. art. 15-3-1 créé par la loi du 23 mars 2019 *(ibid.)*.
[78] Magistrats, greffiers, avocats, huissiers et experts – Officiers de Police judiciaire dans le cas de la procédure pénale.
[79] VERGES Etienne, *Réforme de la procédure pénale : une loi fleuve, pour une justice au gré des courants. A propos de la loi n°2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice*, LexisNexis, Droit pénal n°5, mai 2019, étude 12, al.17 : « […] numérisation dont on espère qu'elle se concrétisera un jour […] en permettant l'accès au dossier pénal sur une plateforme de consultation en ligne. »

51. La doctrine s'accorde à dire que cette numérisation des informations et des échanges modifie la façon d'exercer le droit pénal, au motif qu'elle influence de manière importante la défense pénale[80], ainsi que l'administration de la justice pénale[81].

52. La dématérialisation du support administratif des procédures. – Cette adaptation de la procédure pénale à la numérisation de notre société crée un véritable « dossier pénal numérisé[82] ». Les données qui en résultent sont le support administratif d'une procédure et leur rôle est de contribuer au bon déroulement de celle-ci. Néanmoins, ces données, même si elles sont au cœur de la procédure pénale, ne sont qu'un aspect des effets de la numérisation de notre société sur le droit pénal processuel.

b. La dématérialisation des investigations

53. La finalité des investigations numériques. – Au sein de la procédure pénale, le second effet de la numérisation de notre société touche le cœur de l'enquête, en dématérialisant la recherche d'une partie des éléments permettant à une procédure de converger vers la manifestation de la vérité[83]. Les investigations numériques participent à la recherche de tels éléments. Même si une part importante de la présente étude[84] est consacrée à définir avec précision cette notion « d'investigation numérique », une vision macroscopique l'associe intuitivement à la recherche d'informations numériques, à savoir des données[85]. Or, différentes catégories de données doivent être distinguées.

54. Les différentes catégories d'investigations numériques. – En premier lieu, l'enquête pénale permet d'investiguer sur des données qui sont générées par les personnes visées par l'enquête[86], soit intentionnellement *(α)*, soit à leur insu *(β)*.
En second lieu, les investigations numériques consistent à travailler sur des données créées par les autorités judiciaires *(γ)*.

---

[80] SONTAG KOENIG Sophie, *Technologies de l'information et de la communication et défense pénale*, Thèse soutenue le 13 décembre 2013, publiée aux Editions mare et martin, 2015.
[81] TOURE Aminata, *L'influence des nouvelles technologies dans l'administration de la justice pénale,* Thèse soutenue le 8 décembre 2015.
[82] *Ibid.* SONTAG KOENIG Sophie, *Technologies de l'information et de la communication et défense pénale*, p.124.
[83] V. *supra* n°1.
[84] V. *infra* n°104. et s.
[85] V. *supra* n°7.
[86] Suspect, témoin, entourage d'un suspect ou d'une victime, etc.

α. Les données générées intentionnellement par les personnes ciblées par l'enquête

55. Le numérique « au service » des activités délictuelles et criminelles. – Pour comprendre l'enjeu de l'accès, par les enquêteurs, aux données générées par les protagonistes intéressant une procédure pénale, il est nécessaire de revenir sur la vision des sociologues. Ces derniers analysent la numérisation de notre société comme modifiant les vecteurs de communication et, surtout, contribuant à accélérer les échanges au sein des réseaux sociaux auxquels appartient une personne[87].

56. Or, le délinquant ne peut pas se passer de cette célérité au sein du réseau social auquel il appartient pour mener à bien ses activités délictuelles ou criminelles. Il génère alors des données, au travers de ses échanges et de l'utilisation des objets communicants tels que ceux qui ont envahi la vie quotidienne.

57. La génération intentionnelle des données. – Lorsqu'un individu procède à des recherches sur Internet, ou qu'il échange sur des réseaux sociaux, que ce soit depuis un ordinateur ou depuis un smartphone, il génère une multitude de fichiers temporaires qui pourront permettre, ultérieurement, de découvrir les contenus consultés ou échangés.
Le GPS d'un véhicule enregistre également un historique et d'autres données techniques qui peuvent potentiellement être exploités pour établir les déplacements réalisés. Parfois, les données générées par l'utilisation d'un outil numérique sont enregistrées, non pas sur le terminal utilisé par l'individu, mais sur une plateforme informatique appartenant à un tiers. C'est le cas avec le téléphone, pour lequel l'historique des appels est stocké chez l'opérateur du réseau de téléphonie. L'utilisation d'une montre connectée qui compte les pas va, également, envoyer des données sur une plateforme qui centralise ces informations. Or, quel que soit l'outil utilisé, il existe de nos jours, une importante sensibilisation de tous, sur le fait que l'utilisation d'outils numériques, génère des données à caractère personnel[88]. En conséquence, un utilisateur ne peut pas ignorer qu'il laisse des traces numériques lorsqu'il utilise de tels outils. C'est pourquoi il convient de parler de génération intentionnelle de données, au travers de l'utilisation d'objets numériques ou de logiciels ou, à tout le moins, de données générées en toute connaissance de cause.

[87] V. *supra* n°19. et s.
[88] V. les nombreuses préconisations éditées par la CNIL sur les cookies (« Si vous souhaitez limiter vos traces, il est recommandé de les [les cookies] refuser par défaut. » www.cnil.fr/fr/cookies-les-outils-pour-les-maitriser), sur l'utilisation d'objets connectés, les véhicules connectés, etc. Source : www.cnil.fr

58. Un premier enjeu pour les investigations numériques. – Se pose alors naturellement le problème, pour les autorités judiciaires, de pouvoir accéder à ces données, générées intentionnellement par un utilisateur. L'objectif est de rechercher des preuves parmi ces fichiers ou ces traces numériques et, pour ce faire, de pouvoir utiliser, légalement, des outils techniques permettant d'y parvenir.

59. Des actes de procédure pour accéder aux données. – Pour que les enquêteurs puissent exploiter les données personnelles intentionnellement générées par un individu, cela suppose qu'ils puissent, par exemple, étudier le contenu de son ordinateur ou de son téléphone ou, encore, obtenir ou accéder à des données déposées chez un tiers[89] par la personne qui fait l'objet des investigations.
En conséquence, la procédure doit s'adapter pour faire face à la multiplication des sources contenant des données susceptibles d'intéresser une enquête. Pour cela, de nouveaux actes doivent être créés pour pouvoir légalement accéder à ces données.

60. Une création épisodique et régulière d'investigations numériques. – Cette modification de la procédure pénale pour permettre l'accès à des données personnelles et leur exploitation se réalise au gré de textes successifs[90]. Il existe toujours un temps de retard compréhensible entre l'apparition de nouveaux outils générant des données et la création d'un acte en procédure permettant aux enquêteurs de travailler sur ces informations, puisqu'il est évident que la grande délinquance et les réseaux terroristes s'intéressent également à toutes les innovations technologiques qui pourraient leur être utiles dans leurs activités délictuelles ou criminelles.
De plus, les pouvoirs publics sont tributaires du degré de maturité de ces technologies, ainsi que du temps légitime qu'il faut pour se rendre compte de l'intérêt que pourraient tirer les autorités judiciaires à accéder à certaines données générées par des délinquants, utilisateurs d'outils numériques. Ce fut le cas avec la légalisation de l'utilisation des IMSI-catcher[91] . En effet, la grande criminalité se protège des écoutes téléphoniques en

[89] Il s'agit, notamment, de la faculté de pouvoir accéder aux espaces de stockage en ligne que tous les fournisseurs d'accès à Internet intègrent à leurs offres. V. *infra* n°790.
[90] Ces dernières années, dans le contexte de risque terroriste, il y a eu une accélération de la promulgation de nouvelles lois allant dans ce sens. Celles-ci, souvent prises en réaction aux attentats entre 2016 et 2017, contiennent des modifications relatives à l'exploitation des données personnelles au sein des enquêtes.
[91] V. *infra* n°553.

multipliant l'utilisation de cartes téléphoniques prépayées. Les IMSI-catcher permettent de répondre à cette contrainte.

61. Parfois, le législateur s'y reprend à plusieurs reprises pour une seule et même investigation numérique. En effet, l'utilisation d'une technique telle que prévue par un premier texte, peut ultérieurement révéler l'intérêt qu'il y aurait à l'utiliser différemment ou avec plus de latitude, afin d'augmenter le potentiel de recherche de preuve. Une modification lors d'un texte postérieur est alors nécessaire comme dans le cas de la captation des données informatiques[92]. Dans sa version antérieure à la loi du 3 juin 2016[93], cette investigation numérique ne permettait de capter que les données telles qu'elles s'affichaient à l'écran d'un utilisateur ou que celui-ci les saisissait dans le système. Depuis la loi de 2016, les enquêteurs peuvent accéder à toutes les données stockées dans l'ordinateur cible de la mesure.

62. La difficulté de créer des actes homogènes. – La création de nouveaux actes épisodiquement, souvent au sein de lois au large spectre, a pour conséquence d'engendrer des investigations sans aucune homogénéité par apport à leur appréhension des données. Ce manque de rationalisation se traduit par une multitude de régimes différents pour les mesures mettant en œuvre des investigations numériques[94].

63. Le premier enjeu des investigations numériques[95] consiste donc à ce que des actes de procédure soient créés pour que les enquêteurs puissent accéder, de manière encadrée, aux données générées intentionnellement par les personnes ciblées par l'enquête.

64. Des actions légalement autorisées pour constater. – Beaucoup d'actes de police reposent sur des actions interdites par principe, comme le fait de pénétrer chez autrui pour fouiller[96], le fait de priver une personne de sa liberté le temps d'une garde à vue, etc. Dans le cas de certaines investigations numériques, la situation est similaire, puisque les enquêteurs sont susceptibles de commettre, par eux-mêmes, des faits tombant sous le coup d'une infraction. Un régime d'exception est alors prévu. C'est le cas avec l'enquête

[92] V. *infra* n°570.
[93] 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.
[94] V. *infra* n°233. et s.
[95] V. *supra* n°58.
[96] C. pr. pén. art. 56 : perquisition en enquête de flagrance.

sous pseudonyme[97]. L'agent infiltrant un groupe de discussion est autorisé, en réponse à une demande provenant d'un tiers, à transmettre des contenus illégaux tels que des images pédopornographiques[98].

65. Des outils numériques légalement autorisés pour accéder aux données. – Néanmoins, dans le cas des investigations numériques, il existe une particularité car, pour certains actes d'enquête, ce n'est pas l'action elle-même qui est interdite dans les règles de droit générales, mais l'utilisation d'outils numériques particuliers. Ainsi, pour mener à bien de tels actes, le cadre légal qui les crée doit inextricablement être associée à l'encadrement juridique de l'utilisation ou de la manipulation des outils techniques permettant de mener à bien la mesure d'investigation. En effet, dès lors qu'un acte d'investigation numérique impose l'emploi d'outils dont l'utilisation, voire la simple détention, est, par principe, prohibée sous peine de sanctions pénales, la loi doit lever la présente difficulté. C'est le cas avec la captation de données[99] ou avec la sonorisation et la fixation d'images de certains lieux ou véhicules[100]. La détention de caméras ou de micros espions est punie[101]. L'article 706-98 lève cette difficulté en autorisant explicitement les forces de l'ordre à détenir « les appareils relevant des dispositions de l'article 226-3 du code pénal[102] ».

66. Conclusion du premier enjeu. – Le premier enjeu des investigations numériques consiste à offrir aux autorités judiciaires la possibilité d'accéder à des données générées intentionnellement par les utilisateurs[103], mais l'influence de la numérisation sur les techniques d'enquête crée d'autres besoins.

---

[97] DUMENIL Gabriel, *La nécessité urgente d'encadrer procéduralement la mesure de cyber-infiltration, LexisNexis,* Droit pénal n°9, septembre 2018, étude n°22 : La cyber-infiltration « est dérogatoire en ce qu'elle autorise les agents à commettre certaines infractions. » – V. *infra* n°468.
[98] Ces faits, dans un contexte usuel, tombent sous le coup de l'art. 227-23 al. 2 du C. pén.
[99] C. pr. pén. art. 706-102-1 et s.
[100] C. pr. pén. art 706-96 et s.
[101] C. pén. art. 226-3 : « La fabrication, l'importation, la détention, l'exposition, l'offre, la location ou la vente d'appareils ou de dispositifs techniques […] ayant pour objet la captation de données informatiques […] » est interdite.
[102] C. pén. art. 226-3 : « La fabrication, l'importation, la détention, l'exposition, l'offre, la location ou la vente d'appareils ou de dispositifs techniques […] ayant pour objet la captation de données informatiques […] » est interdite.
[103] V. *supra* n°57.

β. Les données générées à leur insu par les personnes ciblées par l'enquête

67. La création dissimulée de données par un individu. – Un deuxième enjeu doit permettre aux enquêteurs de récupérer des données que la personne visée par une mesure d'investigation numérique génère à son insu. Ces données n'auraient jamais existé sans la mise en œuvre d'un acte de procédure.

68. Les mesures de surveillance. – Au sein de l'enquête, la mise sous surveillance d'un individu fait partie des techniques permettant d'obtenir, soit des éléments de preuve, soit des informations essentielles pour orienter les investigations. Les conséquences de la numérisation générale de notre société sur la surveillance judiciaire d'une personne sont telles, qu'il est aujourd'hui impossible d'envisager la mise en œuvre d'une telle surveillance sans avoir recours à un, voire plusieurs, dispositifs numériques.

69. Même les techniques d'enquête les plus anciennes, comme la filature ou les « planques » sont désormais quasi-systématiquement associées à des actes d'investigation numérique facilitant le travail des enquêteurs. Dans le cas de la filature, la géolocalisation du véhicule de la personne « suivie » est un apport considérable car elle offre la possibilité aux officiers de police judiciaire de se tenir à une distance plus importante, leur évitant ainsi d'être repérés[104]. Pour les « planques », la sonorisation et la fixation d'image[105] du lieu surveillé permet aux enquêteurs d'observer, non seulement les allers et venues, mais également d'entendre les échanges oraux à l'intérieur d'un bâtiment.

70. La double génération de données par les smartphones. – L'utilisation du téléphone mobile est un cas intéressant. En effet, celui-ci permet désormais de procéder à beaucoup de tâches numériques, autrefois réservées aux ordinateurs : surfer sur Internet, envoyer des mails, échanger sur les réseaux sociaux, etc. A ce titre, il génère naturellement beaucoup de données, souvent précieuses pour les enquêteurs[106]. L'exploitation de ces informations entre dans la catégorie des données intentionnellement générées par un individu. Mais, le téléphone va également pouvoir se transformer en dispositif de surveillance, si les autorités judiciaires procèdent à une « écoute

[104] C. pr. pén. art. 230-32 et s. – V. *infra* n°486.
[105] C. pr. pén. art. 706-96 et s. – V. *infra* n°454. et s.
[106] Par ex. : les données de géolocalisation obtenues par le suivi du téléphone, lorsqu'elles sont demandées par les autorités judiciaires *a posteriori* (V. *infra* n°511.).

téléphonique[107] ». Dès lors, la personne ciblée par la mesure va générer des données sous la forme d'enregistrements audio qui n'auraient jamais existés sans la mesure de surveillance et dont elle n'a évidemment pas connaissance.

71. Conclusion des premiers enjeux des investigations numériques. – Le premier et le deuxième enjeu des investigations numériques doivent permettre aux enquêteurs de pouvoir accéder aux données générées par une personne susceptible de détenir des informations intéressant les faits de la procédure en cours, que ces données aient été créées intentionnellement ou à son insu.
Néanmoins, il ne s'agit que d'une partie des investigations numériques.

γ. Les données générées par les autorités judiciaires

72. Le troisième enjeu des investigations numériques. – La numérisation des environnements professionnels a pour objectif de faciliter le travail des salariés ou des agents, quel que soit le domaine d'activité[108]. L'enquête pénale est évidemment concernée par de tels besoins. Outre l'utilisation d'ordinateurs ou de moyens de communications électroniques, certains nouveaux outils venant au support des activités quotidiennes des autorités judiciaires, constituent des investigations numériques à part entière.

73. Les traitements de données judiciaires. – L'environnement de travail des officiers de police judiciaire doit leur permettre de partager et de centraliser des informations facilement. La dématérialisation de ces informations améliore ce partage et cette centralisation en offrant des possibilités de stockage bien plus importantes.

74. Cette dématérialisation se concrétise par la création de traitements de données à caractère personnel mis à disposition des enquêteurs et des magistrats. L'investigation numérique qui consiste à consulter ces traitements verse au dossier de procédure des informations issues de données. C'est, par exemple, le résultat de la consultation du fichier judiciaire national des auteurs d'infractions sexuelles ou violentes[109] qui révèle instantanément qu'un suspect a des antécédents en matière d'infractions sexuelles.

[107] Appellation usuelle « des interceptions de correspondances émises par la voie des communications électroniques » C. pr. pén. art. 100 et s. – V. *infra* n°528.
[108] V. *supra* n°4.
[109] V. *infra* n°667.

75. Des données au cœur de l'enquête. – Ces informations numériques, à la différence des données générées par des suspects ou des témoins, sont sous le contrôle exclusif des autorités judiciaires. Elles ne doivent pas être confondues ou assimilées aux données qui concourent au support de la dématérialisation du support administratif de la procédure[110] car la consultation et la manipulation des traitements de données judiciaires ont pour objectif de verser au dossier d'enquête des éléments de preuve. Par exemple, la comparaison des empreintes d'un suspect avec le fichier automatisé des empreintes digitales[111] peut fournir une preuve déterminante si celles-ci correspondent à des empreintes retrouvées précédemment sur une arme.

76. Conclusion des conséquences de la numérisation sur les investigations en enquête pénale. – La numérisation de notre société a pour conséquence de dématérialiser les informations et les échanges aussi bien dans la vie privée des personnes que dans les domaines professionnels. L'exercice du droit est évidemment concerné par ces évolutions et, à ce titre, la dématérialisation pénètre les investigations en procédure pénale.
Pour autant, tous les progrès techniques qui accompagnent la dématérialisation ne parviennent pas à intégrer les investigations.

§3. Des verrous aux progrès techniques de la numérisation

77. Des évolutions technologiques freinées. – La dématérialisation de notre société et tout particulièrement des domaines professionnels, repose sur un ensemble d'évolutions technologiques. Certaines de ces évolutions ne parviennent pas à intégrer les investigations numériques, alors qu'elles seraient une source d'amélioration aussi bien de l'efficacité de l'enquête que du respect des libertés individuelles.
En premier lieu, les données recueillies ou générées lors de l'exécution des différents actes d'investigation numérique ne bénéficient pas des techniques récentes qui permettent une exploitation optimisée des données de masse *(I)*.
En second lieu, les données mettant en œuvre les traitements de données judiciaires restent physiquement séparées, alors que les techniques de regroupement des données communes à plusieurs traitements optimisent la qualité et la protection des informations numériques collectées *(II)*.

[110] V. *supra* n°43. et s.
[111] V. *infra* n°661.

I – Le verrou du cloisonnement des données issues des investigations numériques

78. Deux difficultés cumulatives. – L'application des techniques d'exploitation des données de masse[112] aux informations numériques collectées au travers des actes d'investigations se heurte à deux difficultés. La première, intrinsèque, est incompatible, avec la séparation des actes d'enquête au sein de la procédure pénale.

De plus, une seconde difficulté, cumulative, apparaît. En effet, il existe actuellement une impossibilité de lister l'ensemble des investigations numériques offertes aux autorités judiciaires par la procédure pénale. Cette impossibilité empêche d'identifier exhaustivement les données issues d'actes d'enquête qui pourraient être regroupées afin d'en optimiser l'exploitation.

C'est pourquoi, pour comprendre les difficultés d'intégrer les techniques d'exploitation des données de masse aux investigations numériques, il est nécessaire de distinguer l'incompatibilité entre le regroupement des données issues des actes d'enquête et le principe de séparation des actes *(A)* et l'impossibilité de lister l'ensemble des données susceptibles d'être concernées par un tel regroupement *(B)*.

A. L'impossible conciliation du regroupement des données avec le principe de séparation des actes de procédure

79. La séparation des actes de procédure comme première difficulté. – L'enquête en procédure pénale fonctionne avec des mesures qui sont exécutées indépendamment les unes des autres. Bien sûr, cela ne fait pas obstacle au fait qu'un acte d'investigation puisse être réalisé en fonction du résultat d'une mesure précédemment exécutée. C'est notamment le cas lorsqu'une perquisition permet de trouver la présence d'une trace ADN. Si l'individu à qui elle appartient est connu dans le fichier national automatisé des empreintes génétiques, il est alors identifié et une mesure découlant directement de cette constatation peut être ordonnée. Par exemple, son téléphone peut être mis sur écoute.

Néanmoins, la procédure pénale repose sur des actes d'enquête qui se terminent par la remise d'un rapport ou d'un procès-verbal, même s'il existe des liens entre certains actes d'investigation tels que ceux qui viennent d'être évoqués.

80. Le passage obligatoire par un rapport ou un procès-verbal. – Le rapport ou le procès-verbal qui clôture un acte, a une conséquence importante lorsqu'il s'agit

[112] V. *infra* n°762.

d'investigations numériques. Il est l'une des sources du verrou à l'intégration des techniques d'exploitation de masse des données collectées au travers des actes d'enquête. Par exemple, les investigations diligentées sur un ordinateur saisi lors d'une perquisition vont se dérouler dans le cadre d'une expertise[113]. Au terme de sa mission, l'expert commis remettra au juge un rapport, accompagné de l'ordinateur qu'il aura replacé sous scellés à la fin de ses investigations. Si, ultérieurement, une personne est soupçonnée et que les officiers de police judiciaire, dans le cadre d'une commission rogatoire, saisissent son téléphone portable, ils vont procéder à des investigations sur celui-ci en ayant uniquement accès au rapport de l'expert précédemment évoqué[114]. Ainsi, ils n'ont pas accès, au titre de l'acte permettant les investigations dans le téléphone, aux données contenues dans l'ordinateur précédemment exploité.

81. L'apport potentiel des techniques des données de masse. – Cette rupture dans la continuité des données saisies ou collectées par les différents actes de procédure nuit à l'efficacité de l'enquête. En effet, dans le cas précédent, les investigations sur les données contenues dans le téléphone, ajoutées aux données présentes dans l'ordinateur objet de l'expertise seraient potentiellement beaucoup plus efficaces grâce aux techniques d'analyse des données de masse (le *big data*[115]) qui sont actuellement en plein développement[116]. Ces techniques reposent sur le développement de l'intelligence artificielle qui, notamment, réalisent des corrélations automatiques d'informations. En enquête pénale, ce pourrait être des preuves numériques que les algorithmes informatiques révèlent alors que l'intelligence humaine ne pourrait pas procéder au recoupement d'une masse énorme de données, ou dans un laps de temps démesurément long.

82. L'enjeu de l'analyse regroupée de toutes les données recueillies lors des différentes investigations. – Un travail fondamental a pour objectif d'améliorer la part de l'enquête procédant à des investigations sur les données. L'enjeu consiste à lever le verrou qui vient d'être décrit afin de parvenir à concilier le principe de séparation des

[113] V. *infra* n°301.
[114] L'ordinateur ayant fait l'objet de l'expertise a été replacé sous scellés par l'expert et remis au juge conjointement à son rapport.
[115] V. *infra* n°766.
[116] V. *infra* n°766.

mesures d'enquête[117] avec le besoin, pour les enquêteurs, de pouvoir accéder aux données exploitées lors d'actes précédents et déjà terminés, pour des investigations diligentées sur de nouveaux supports numériques saisis lors de mesures en cours d'exécution.

B. L'impossibilité de lister l'ensemble des données susceptibles d'être regroupées

83. Une deuxième difficulté au travers de la nécessité d'identifier les actes exploitant des données. – Une difficulté supplémentaire découle directement de l'adaptation du droit processuel à la numérisation de notre société qui s'opère épisodiquement[118], sans aucun souci de cohérence au sein des investigations numériques.
Quelles sont les données qui devraient être regroupées ?
Cette question revient à en poser une autre : quels sont les actes d'enquête qui devraient autoriser une exploitation étendue des éventuels scellés auxquels ils aboutissent ?

84. La difficulté d'identifier les actes concernés. – Outre la difficulté de définir avec précision la notion d'investigation numérique[119], il est, en l'état actuel, impossible de dresser une liste exhaustive de toutes les mesures susceptibles d'être exécutées en enquête et conduisant à recueillir, manipuler ou générer des données.
Cette impossibilité trouve sa principale origine dans la difficulté qui existe, y compris dans la doctrine, de classer les investigations.

85. Le rattachement des investigations numériques à la preuve en procédure pénale. – Pour la doctrine, les investigations numériques sont des investigations comme les autres. Or, certains auteurs[120] décrivent les actes d'investigations lors de l'étude des différentes phases préparatoires[121]. Cette façon de procéder semble mal adaptée aux investigations numériques car elles sont identiques ou très proches, qu'elles soient mises en œuvre en enquête ou lors de l'information judiciaire. Cela rend donc leur présentation fortement répétitive.

---

[117] V. *infra* n°755.
[118] V. *supra* n°60.
[119] V. *supra* n°53.
[120] LEROY Jacques, *Procédure pénale,* 4ème édition, LGDJ : les actes d'investigations sont présentés au travers de l'enquête de police et ensuite lors de l'instruction préparatoire avec les « actes d'instruction ».
CONTE Philippe et LARGUIER Jean, *Procédure pénale,* 24ème édition, Dalloz : *idem*. Les actes sont présentés à la fois avec « les opérations de police judiciaire » et dans le cadre « des pouvoirs et des devoirs du juge d'instruction ».
[121] Enquête préliminaire, de flagrance et information judiciaire.

86. Une autre partie de la doctrine[122] fait un choix différent en commentant les actes d'investigations au sein de l'étude de la preuve pénale. Cette méthode correspond bien aux investigations numériques car elle permet de les étudier en s'appuyant sur leur finalité qui, en l'occurrence, consiste à obtenir des preuves qui reposent sur des données informatiques.

87. Toutefois, « le Code de procédure pénale ne comporte pas de théorie générale de la preuve[123] » même si le mot y est régulièrement employé. L'étude de la preuve, en revanche, renvoie au cadre légal de l'administration de la preuve. Cette notion est différente de la preuve en elle-même, puisque « elle est l'opération intellectuelle par l'effet de laquelle un fait est censé être vrai et peut fonder une condamnation »[124].

88. Une absence de classement préjudiciable. – Ainsi, les mesures permettant de mettre en œuvre des investigations numériques font partie de l'administration de la preuve, ce qui ne débouche sur aucune classification logique et rationnelle de tous les actes permettant de procéder à des investigations. De plus, certains auteurs affirment qu'un tel classement est inutile et qu'il faut considérer les actes d'investigations dans leur ensemble comme un « répertoire dans lequel [les] agents doivent choisir pour la recherche et le recueil des indices[125] ».

89. L'absence de tout classement des investigations en général induit, évidemment, une absence de classement des investigations numériques. Ainsi, l'impossibilité qu'il existe actuellement de pouvoir recenser l'ensemble des actes concourant à recueillir ou générer des données est un verrou qui doit être levé, préalablement à l'étude visant à proposer une exploitation des données regroupées, issues de différentes mesures d'enquête.

---

[122] PRADEL Jean, *Procédure pénale*, Collection Référence, 18ème édition, Edition Cujas : les investigations sont présentées dans un titre relatif aux « objets essentiels de la phase préparatoire » au travers de plusieurs chapitres (« la preuve de l'acte » et « la connaissance des personnes »).
VERGES Etienne, *Procédure pénale,* 4ème édition, LexisNexis : les investigations sont présentées dans un chapitre relatif « au modes de preuve », même si certains actes sont distingués au sein de l'enquête et de l'instruction.
[123] BOULOC Bernard, *Procédure pénale,* 24ème édition, Dalloz : page 111.
[124] PRADEL Jean, *Procédure pénale*, *ibid* : page 363.
[125] GUINCHARD Serge et BUISSON Jacques, *Manuel de Procédure pénale*, LexisNexis, 10ième édition, pages 525 et s.

II – Le verrou de la séparation des données constituant les traitements judiciaires

90. La dématérialisation d'informations hautement sensibles. – L'un des principaux effets de la dématérialisation est de créer des traitements de données à caractère personnel. Le nombre de fichiers directement accessibles aux autorités judiciaires lors d'une enquête pénale est en constante augmentation[126]. De par le caractère éminemment sensible des informations collectées et enregistrées dans le cadre des procédures pénales, ces bases de données judiciaires suscitent souvent l'inquiétude de la population[127].

91. Une multitude de traitements distincts. – Face à cette inquiétude, la réponse des autorités publiques est de multiplier les bases de données judiciaires, en séparant physiquement les données qui les composent. Par exemple, le traitement d'antécédents judiciaires[128] est mis en œuvre par la Gendarmerie et la Police nationale et est placé sous la responsabilité du Ministère de l'intérieur. Dans le même temps, le fichier judiciaire national automatisé des auteurs d'infractions sexuelles ou violentes[129] et le fichier judiciaire national automatisé des auteurs d'infractions terroristes[130] sont sous l'autorité du Ministère de la justice et sont opérationnellement tenus par le service du Casier judiciaire.

92. L'apport potentiel des techniques des bases de données sensibles. – Or, la sécurité informatique qui entoure les bases de données est une préoccupation majeure des pays occidentaux depuis plusieurs années, induisant de nombreux travaux visant à sécuriser les systèmes d'information et les échanges de données. Les techniques informatiques et organisationnelles qui en découlent permettent de créer des bases de données importantes, avec une gestion très fine des droits d'accès aux différentes données.

93. Une séparation inutile et dangereuse. – La gestion par les autorités publiques de traitements de données physiquement séparés est un verrou pour que ces techniques de sécurisation et d'amélioration de la qualité des informations collectées puissent bénéficier aux traitements judiciaires. Une telle séparation se voudrait plus protectrice des personnes fichées alors, qu'au contraire, elle nuit au respect des libertés individuelles. En

[126] V. *infra* n°630.
[127] V. *infra* n°969. et n°970.
[128] V. *infra* n°641.
[129] V. *infra* n°667.
[130] *Ibid.*

effet, il est plus difficile de procéder à des contrôles de la conformité du bon usage qui est fait des informations, avec une multitude de fichiers qu'avec une seule base de données[131]. De plus, la multiplication des fichiers a pour effet de créer une redondance d'informations identiques dans des fichiers de police différents[132], ce qui nuit à leur mise à jour et donc, par voie de conséquence, aux respects des droits en matière de données personnelles dont la fiabilité des informations stockées est primordiale.

94. L'enjeu de la consolidation des traitements judiciaires. – Une part importante de la présente étude consiste à étudier les conditions et les effets d'un regroupement des données constituant les traitements de données judiciaires. Il y a là un enjeu important car une telle consolidation améliorerait considérablement le respect des libertés individuelles : un meilleur contrôle, des informations plus fiables, ou encore des accès mieux encadrés.

* * *

* *

95. Une étude pour lever les verrous au déploiement de nouvelles techniques numériques au service de l'enquête en procédure pénale. – L'enquête au sein de la procédure pénale ne bénéficie actuellement pas de toutes les innovations, *a priori* positives, qui découlent de la numérisation de notre société. Un enjeu considérable consiste donc à étudier comment il est possible d'intégrer certains de ces progrès technologiques, en évitant d'envisager des chamboulements processuels qui ne seraient pas réalistes. Une partie de cet objectif impose de préserver l'équilibre de la procédure pénale entre l'efficacité offerte au pouvoir d'enquête et le respect des libertés individuelles. En effet, dans le contexte de numérisation qui vient d'être décrit, tout acte permettant d'investiguer dans les données personnelles d'une personne, ou toute collecte massive de données mise en œuvre par les autorités judiciaires, est nécessairement fortement intrusif.

96. La nécessité de définir et d'identifier les investigations numériques. – Cependant, pour être en mesure de procéder à une telle étude, le prérequis indispensable

[131] V. *infra* n°1025.
[132] Par ex. l'adresse, les coordonnées téléphoniques, les antécédents, etc.

est d'être en mesure d'identifier avec précision ce qui entre dans le périmètre des investigations numériques. En effet, les actes d'enquête susceptibles de déclencher une investigation numérique sont totalement éparpillés dans le Code de procédure pénale, et il convient de les identifier clairement afin de pouvoir en étudier les régimes actuels.

97. C'est la raison pour laquelle, les investigations numériques doivent être définies et exhaustivement identifiées malgré leur éparpillement dans le Code de procédure pénale *(première partie),* avant que les avantages du regroupement des données qui sont le fruit de ces investigations ne puissent être étudiés *(seconde partie)*.

PREMIERE PARTIE.
LE CONSTAT DE L'EPARPILLEMENT DES INVESTIGATIONS NUMERIQUES

98. Le flou autour de la notion « d'investigation numérique ». – Intuitivement, l'appellation « investigation numérique » établit un lien avec les données informatiques. Néanmoins, il ressort de la doctrine que les auteurs ne positionnent pas tous ce lien à l'identique[133]. Certains voient dans l'investigation numérique un acte d'enquête utilisant des outils technologiques au sens large, tandis que d'autres considèrent qu'une investigation est numérique si elle concerne un environnement informatique.
Ces différents positionnements du rapport à la donnée révèlent plusieurs ambiguïtés autour de ce qu'est réellement une investigation numérique en procédure pénale. En conséquence, une définition précise doit être posée.

99. Des investigations numériques éparpillées. – Nonobstant cette absence d'une définition précise, la vision intuitive des investigations numériques suffit à constater qu'elles sont totalement éparpillées dans le Code de procédure pénale.
100. Une création continue et régulière d'investigations numériques. – Cet éparpillement trouve sa source originelle dans l'une des adaptations de la procédure pénale à la numérisation de notre société : la dématérialisation de certaines investigations[134].

[133] V. *infra* n°148.
[134] V. *supra* n°53.

Pour ce faire, la procédure s'adapte par la création d'actes permettant aux enquêteurs de recueillir, manipuler ou générer des données dont la finalité est de verser des éléments de preuve au dossier d'enquête.

Cette adaptation se fait de manière continue, par étapes successives au travers de textes ponctuels, en fonction des évolutions et de l'apparition de nouveaux outils numériques[135].

101. Une absence de réflexion de fond. – La conséquence de ces modifications épisodiques, distantes dans le temps, est l'absence de réflexion sur l'homogénéité des investigations numériques.

Il résulte de ce manque de réflexion de fond sur la dématérialisation de certaines investigations, une absence de toute logique dans le classement et l'organisation des actes permettant de les mettre en œuvre au sein de la procédure pénale et, par voie de conséquence, une hétérogénéité dans les régimes de ces actes.

102. La nécessité d'un recensement exhaustif. – Cette absence de classement impose de recenser et de cataloguer les investigations numériques, individuellement.

103. Une étude en deux temps. – Pour ce faire, il est préalablement nécessaire de définir précisément la notion d'investigation numérique en procédure pénale *(Titre I)*. Cette définition est indispensable pour identifier l'ensemble de ces investigations afin d'en étudier les régimes correspondants, aussi bien dans les conditions de leur mise en œuvre que dans leurs effets *(Titre II)*.

[135] V. *supra* n°60.

TITRE I. LA NECESSITE DE DEFINIR LA NOTION « D'INVESTIGATION NUMERIQUE »

104. Le constat d'une absence de définition. – Outre l'impossibilité de définir les investigations numériques à partir du Code de procédure pénale, en raison d'une absence de tout classement logique des actes permettant de les mettre en œuvre, l'expression « investigation numérique » est peu utilisée dans la doctrine juridique. Souvent, d'autres expressions, plus percutantes telles que « perquisitions 2.0 » ou « preuve électronique » lui sont préférées[136]. Néanmoins, ces dernières présentent le défaut de ne couvrir qu'une partie des investigations numériques et ne permettent donc pas de les définir. Chez les informaticiens, l'expression est plus fréquemment utilisée mais sans qu'une définition satisfaisante se dégage de l'usage qui en est fait.

105. La nécessité de combler l'absence de définition. – Une analyse de la perception pluridisciplinaire et « grand public » de l'investigation numérique, révèle qu'il n'existe pas, à l'heure actuelle, de véritable définition ou, en tout état de cause, de définition permettant de répondre aux exigences d'un concept juridique précis *(Chapitre 1)*.

Dès lors, cette notion doit être précisée au travers de critères précis permettant de circonscrire parfaitement ce qu'est une investigation numérique *(Chapitre 2)*.

[136] SONTAG KOENIG Sophie, *Les perquisitions 2.0 : quand l'informatique se saisit de l'immatériel,* Dalloz AJ Pénal 2016 p.238.
MICHALSKI Cédric, *La recherche et la saisie des preuves électroniques*, Gazette du Palais 11 fév. 2014 n°42 p.12.

Chapitre 1. L'absence de définition de l'investigation numérique

106. L'erreur d'une appréhension superficielle. – La notion « d'investigation numérique » est perçue, à tort, comme une évidence. Tout d'abord, l'erreur repose sur une mauvaise perception du mot « numérique ». En effet, celui-ci est devenu une telle évidence pour notre société qu'il semble que, même dans la doctrine, personne n'a réellement éprouvé le besoin de le définir rigoureusement, sans s'interroger sur les nuances pourtant non négligeables, voire même parfois les différences qui existent entre des mots tels que « digital », « électronique » et « numérique ». Ensuite, l'erreur d'une compréhension trop superficielle provient d'une tentative de définition de l'investigation numérique par son objet, décrit parfois à tort de manière trop limitative, comme consistant uniquement à produire des preuves numériques.

107. En conséquence, la mauvaise perception du mot « numérique » doit être constatée *(Section 1)*, tout comme le rapprochement erroné qui est fréquemment opéré entre « investigation numérique » et « preuve numérique » *(Section 2)*.

Section 1. L'erreur d'une définition perçue comme évidente

108. Le constat de l'incertitude. – L'appellation « investigation numérique » est une notion dont la compréhension est considérée comme évidente par ceux qui l'emploient, qu'ils soient juristes, techniciens ou parmi le grand public. Pourtant, de nombreuses interrogations et ambiguïtés apparaissent lorsque sont étudiées les utilisations concrètes de l'emploi qui est fait de cette appellation. Il en résulte des imprécisions incompatibles avec la complétude qu'exige une notion juridique conceptuelle. Ces imprécisions se dégagent aussi bien de l'étude de l'association des deux mots « investigation » et « numérique » pris individuellement *(§1)*, que de celle de l'expression « investigation numérique » dans son ensemble *(§2)*.

§1. Les mots « investigation » et « numérique »

109. L'étude des mots pris isolément. – Les définitions des deux mots séparés révèlent que l'utilisation du mot « investigation » dans la doctrine juridique est en adéquation avec la définition littéraire. La situation devient plus délicate avec le mot « numérique ». En effet, historiquement, le législateur a préféré le mot « électronique » dans un emploi à contre-sens de la définition littéraire et technique de ce mot. Il en résulte de profondes ambiguïtés pour toutes les dispositions légales ou règlementaires ou articles des auteurs de la doctrine juridique, qui concernent la dématérialisation des informations et des actes.

110. Ainsi, l'étude du mot « investigation » révèle une stabilité *(I)*, contrairement à « numérique » qui est une source d'importantes ambiguïtés *(II)*.

I – La stabilité de la notion « d'investigation »

111. Une définition plus vaste que la perception courante. – Les dictionnaires définissent le mot « investigation » comme l'action de rechercher attentivement quelque chose[137], ce qui en fait une acception plus vaste que la recherche des preuves. Dans l'esprit du grand public, pourtant, ce mot est perçu de manière plus restrictive car il est systématiquement assimilé à la connotation d'enquête[138].

112. La doctrine juridique en phase avec la définition littéraire. – En matière civile, les auteurs utilisent le mot au travers du « pouvoir d'investigation du magistrat[139] », puisque celui-ci est fortement limité et contraint par le respect du contradictoire et par la conception accusatoire de la procédure. Le juge ne dispose donc que de « mesures d'investigation » encadrées par les textes[140]. Ici, le mot « investigation » couvre une recherche d'éléments qui ne peuvent pas tous être qualifiés de preuve[141]. Par exemple, le

[137] V. le dictionnaire Littré qui définit le mot « investigation » par « l'action de suivre à la trace, de rechercher attentivement », ou le Larousse avec « investiguer » : « faire une recherche attentive et suivie ».
[138] V. les émissions diffusées sur les chaînes de télévision comme « Cash investigation » sur France 2, ou encore, à Radio France, le service « Enquêtes-investigations » au sein de la rédaction.
[139] V. par ex. MOURALIS Jean-Louis, *Preuve – Chapitre 3 – Recherche et appréciation des preuves*, Répertoire de droit civil, Dalloz, al. 557 : il s'agit du pouvoir souverain dont dispose le juge pour ordonner des investigations demandées par l'une des parties. En effet, le juge n'est pas obligé de l'ordonner s'il la considère inutile.
[140] GOUTTENOIRE Adeline et FULCHIRON Hugues, *Autorité parentale – Titre 2 Exercice de l'autorité parentale*, Répertoire de droit civil, Dalloz, al. 304 et s.
[141] Sur la notion de preuve, v. *infra* n°158.

juge aux affaires familiales peut ordonner des expertises psychologiques[142] dont le résultat n'est pas à proprement parler une preuve. Pour autant, le juge va s'appuyer sur de tels éléments, qui sont le résultat d'actes rattachés à son pouvoir d'investigation, pour rendre une décision.

113. Pour les pénalistes, le mot « investigation » est, non seulement fréquemment utilisé, mais également de manière très transversale à toute la procédure puisqu'il est fait référence à l'investigation jusque dans l'application des peines, sans qu'il soit question de rechercher, à ce stade, des preuves[143].

114. Une recherche d'éléments au sens large. – Hormis une interprétation parfois trop restrictive qui consiste à associer le mot « investigation » à la recherche des preuves, l'usage qui est fait de ce terme dans le vocabulaire juridique ne soulève pas de difficulté. Dans le cadre d'une procédure judiciaire, il s'agit de rechercher des éléments avec une large finalité, qui permettent de faire avancer un dossier vers une solution.

II – La confusion autour de « numérique »

115. Une fausse synonymie dans le vocabulaire juridique. – Si le mot « investigation » se caractérise par une stabilité de l'usage qui en est fait, il n'en est pas de même avec le terme « numérique ». Le vocabulaire juridique lui préfère souvent, à tort, le mot « électronique », générant une confusion dont les répercussions touchent directement la définition des investigations numériques.

116. La clarté de la définition informatique de « numérique ». – La définition littéraire du mot « numérique[144] » explicite qu'il s'agit d'informations codées sous la forme de données binaires[145], c'est-à-dire exploitables dans un environnement informatique.

---

[142] *Ibid*. MOURALIS Jean-Louis. Il peut s'agir d'expertises médico-psychologiques ou d'enquêtes sociales qui sont prévues et encadrées par le Code civil : v. art. 376-2-11 et 373-2-12.

[143] FAUCHER Pascal, *Juridictions de l'application des peines – Conditions de recevabilité, investigations, expertises, moyens de contraintes*, procédure pénale, JurisClasseur, Fasc. 30 : « Les juridictions de l'application des peines ont été dotées de pouvoirs d'investigation importants permettant la recherche d'informations ou du condamné. »

[144] V. dictionnaire Larousse : « Se dit de la représentation d'informations ou de grandeurs physiques au moyen de caractères, tels que des chiffres, ou au moyen de signaux à valeurs discrètes. »

[145] Un bit est l'unité élémentaire de l'information en informatique, ne pouvant prendre que deux valeurs (0 ou 1).

Techniquement, il est synonyme de « digital » et s'oppose donc à « analogique », qui fait référence à une représentation continue d'une information. Pour devenir numérique, l'information analogique en question doit être échantillonnée, c'est-à-dire transformée en données binaires. Par exemple, la mesure d'une température prise avec un thermomètre est analogique puisque c'est une courbe continue. Pour être exploitable en informatique, il faut transformer cette courbe en données numériques. Ce sont donc des points pris à intervalles réguliers qui donnent la température de manière digitale.

117. L'erreur de l'utilisation du mot « électronique » dans les textes de loi. – Cette opposition entre numérique et analogique n'a pas été comprise par le législateur. Comme précédemment évoqué, le droit civil a pris en compte depuis longtemps la numérisation de notre société[146]. Sur ce sujet, la loi sur la signature électronique[147] et le décret d'application correspondant[148] ont, dès 2000 et 2001, été précurseurs dans ce domaine[149]. Malheureusement, le mot « électronique » a été préféré à « numérique », dans un emploi totalement inapproprié. En effet, « électronique[150] » se réfère aux composants du même nom[151], que l'on retrouve quasiment partout, y compris dans des objets qui ne sont pas numériques. Par exemple, un vieux tourne-disque à vinyle ou un téléphone à touches contient des composants électroniques alors qu'il ne repose en rien sur des technologies digitales. Or, dans les deux textes précités, l'esprit du législateur se réfère clairement à une signature numérique, à savoir dématérialisée.

118. Une continuité dans l'erreur. – Il est dommageable que les dernières évolutions du droit civil persistent dans ce contresens, et n'aient pas opté pour l'utilisation du mot numérique. En effet, la réforme du droit des obligations de 2016 est venue, notamment, supprimer ce qui avait été introduit par la loi du 13 mars 2000 sur la signature

[146] V. *supra* n°27.
[147] Loi n°2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique.
[148] Décret n°2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique. Ce décret a été abrogé et remplacé par le décret n°2017-1416 du 28 septembre 2017 relatif à la signature électronique.
[149] Il aura fallu attendre quatre ans pour avoir un texte complet s'intéressant en profondeur à Internet avec la loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, dite « LCEN ».
[150] V. dictionnaire Larousse. Electronique : « Qui se rapporte à l'électronique ou qui fonctionne suivant ses principes. »
[151] Pour les scientifiques, l'électronique se réfèrent aux composants ou aux systèmes, qui sont des ensembles de composants. Source : Conseil National des Universités, section 63 (Génie électrique, électronique, photonique et systèmes).

électronique, pour la remplacer par un article 1366 du Code civil qui dispose que « l'écrit électronique a la même force probante que l'écrit sur support papier[152] ».

119. Une forte disparité en matière pénale. – La confusion dans l'emploi du mot « électronique » existe également en droit pénal. Pour autant, cette confusion n'est pas la règle, car certaines dispositions utilisent le vocabulaire adéquat.

120. Une mauvaise utilisation des termes. – En premier lieu, l'ambiguïté est présente lorsqu'il est question de « communication électronique », aussi bien pour traiter de la diffusion d'informations[153] que de la transmission de documents comme à l'article 19 du Code de procédure pénale, qui s'intéresse aux échanges entre les officiers de police judiciaire et le Parquet. Celui-ci dispose que « le procureur de la République peut autoriser que les procès-verbaux, actes et documents lui soient transmis sous forme électronique ». L'erreur dans l'utilisation du mot « électronique » atteint ici son paroxysme car les composants électroniques sont très loin de l'idée que le législateur a voulu exprimer. Comme en matière civile, c'est celle de dématérialisation qui habite l'esprit du texte et le mot « numérique » aurait dû être utilisé.

121. Une utilisation adéquate des bons termes. – En second lieu, et *a contrario*, le mot électronique est utilisé à bon escient dans le Code pénal, quand il est question de surveillance électronique[154] ou d'éthylotest électronique[155]. Ici, en effet, il s'agit bien d'outils ou d'instruments, constitués de composants.

122. Il en est de même avec les « interceptions de correspondances émises par la voie des communications électroniques[156] ». Le mot électronique est parfaitement adapté. En effet, même si désormais la quasi-totalité des échanges téléphoniques sont numériques[157], certaines communications peuvent rester analogiques et l'enregistrement de ces conversations peut s'envisager avec un magnétophone à bande. En conséquence, le mot « numérique » n'aurait pas été adapté ici. L'interception des correspondances numériques n'est qu'une partie de l'interception des correspondances en général.

---

[152] *Op. cit.* P.12, l'ordonnance n°2016-131 du 10 février 2016.
[153] V. par ex. C. pén. art. 131-35 au sujet de la publication des décisions judiciaires ordonnées par une juridiction de jugement.
[154] V. par ex. C. pén. art. 132-26-1 et s.
[155] C. pén. art. 132-45.
[156] C. pr. pén. art. 100 et s. « Des interceptions de correspondances émises par la voie des communications électroniques. » V. *infra* n°528. pour une étude de la mesure.
[157] V. *infra* n°536.

123. Toujours dans le Code de procédure pénale, plusieurs dispositions relatives aux procès-verbaux constatant des infractions[158], emploient l'expression « signature numérique ou électronique ». L'utilisation des deux mots est rigoureusement exacte. En matière d'infractions au Code la route, les automobilistes verbalisés signent désormais leur procès-verbal sur un boitier que leur tend l'agent des forces de l'ordre[159]. C'est donc une signature électronique puisqu'elle est faite par la main du contrevenant, mais au lieu d'être portée sur un support papier, elle est réalisée sur un boitier électronique, d'où son nom. On notera que cette signature électronique va donner naissance à une image qui elle, sera numérique par nature. Cependant, le législateur a également prévu la possibilité de procéder à une signature numérique qui est différente d'une signature manuscrite stockée sous forme d'image, et qui doit être comprise comme la signature d'un document via un dispositif informatique identique à celui qui est connu de tous les contribuables réalisant leur déclaration d'impôt en ligne[160].

124. Le décret du 24 mai 2019[161] a créé l'article D589-2 dans le Code de procédure pénale qui est consacré à la signature dématérialisée dans le cadre de la numérisation de la procédure pénale[162]. Cet article est une illustration de la parfaite utilisation de « numérique ». Ces dispositions, complétées par un arrêté de septembre 2019[163], opèrent une juste distinction entre « la signature sous forme numérique » et la « signature manuscrite recueillie sous forme numérique ». Il s'agit, dans ce dernier cas, de la signature qu'un individu réalise « à la main » et qui est, *in fine*, stockée sous forme d'image après une étape de numérisation.

125. De même, l'article 308 relatif à l'enregistrement des débats des Cours d'assises prévoit que « l'enregistrement peut être placé sous scellé numérique […] » ce qui, une nouvelle fois, démontre l'emploi du mot adéquat. En effet, par scellé numérique on

---

[158] C. pr. pén. art. 495-22 et 530-6 : « Pour l'application des dispositions relatives à l'amende forfaitaire, le lieu du traitement automatisé des informations nominatives concernant les infractions constatées par un procès-verbal revêtu d'une signature numérique ou électronique est considéré comme le lieu de constatation de l'infraction. »

[159] Il est toutefois prévu une version « intermédiaire » dans le cas où le dispositif permettant la constatation ne peut pas enregistrer la signature du contrevenant (par exemple pour le stationnement, si le conducteur n'est pas présent ce qui est le cas le plus fréquent) ou ne permet pas l'édition immédiate de l'avis de contravention : v. C. pr. pén. art. A37-15 et s.

[160] Il s'agit de la signature répondant aux exigences initialement prévues par la Loi du 13 mars 2000 *(op. cit.* P.35).

[161] *Op. cit.* p.19. Décret n°2019-507 du 24 mai 2019 pris pour l'application des dispositions pénales de la loi n°2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice relatives à la procédure numérique, aux enquêtes et aux poursuites

[162] V. *supra* n°48.

[163] Arrêté du 6 septembre 2019 fixant les modalités d'application des articles D. 589 et suivants du code de procédure pénale relatifs à la procédure pénale numérique.

imagine que les données correspondant aux enregistrements sont stockées dans un espace de stockage informatique, ce qui se fait, par exemple, au travers d'un mot de passe à usage unique[164], mais, surtout, avec une traçabilité totale[165] qui permettrait immédiatement d'identifier une personne qui y aurait accédé.

126. La réquisition d'un tiers aux fins d'obtenir des informations susceptibles d'intéresser une procédure en cours[166] prévoit, en amont, que cette réquisition puisse être « faite par un moyen de communication électronique[167] » et, lors de son exécution, que le tiers réquisitionné puisse « remettre ces informations, notamment sous forme numérique […] », autrement dit de manière dématérialisée. Le seul fait d'avoir prévu ces possibilités ajoute une grande efficacité potentielle à cet acte de réquisition qui doit être soulignée[168].

127. Conclusion du paragraphe §1 : les mots « investigation » et « numérique ». – L'étude de la définition des deux mots pris isolément révèle qu'une incertitude importante entoure la définition d'une investigation numérique en procédure pénale. Si le mot « investigation » correspond, de manière stable et sans ambiguïté, à une recherche d'éléments concourants à résoudre une procédure pénale, la confusion qui s'est durablement installée chez le législateur et les autorités publiques avec le mot électronique soulève des questions.

128. Dans de nombreux textes, l'emploi à contresens du mot « électronique » comme synonyme de « numérique » ouvre une difficulté pour les investigations. Les investigations numériques peuvent-elles être assimilées à des investigations électroniques ? Si, au sein d'une enquête, une expertise est ordonnée sur un ancien caméscope à bande, il s'agit clairement d'une investigation électronique puisque ce matériel est composé de composants électroniques, mais il ne peut s'agir d'une investigation numérique car aucune donnée informatique n'est contenue dans un tel équipement.

---

[164] Sécurité informatique, *Evidian classe les méthodes d'authentification les plus utilisées*, Sécurité informatique n°352, 24 mai 2011 : « (2) Mot de passe à usage unique (*'one-time password'* - OTP) : L'OTP permet d'éviter qu'un mot de passe soit volé et réutilisé. »

[165] Sur la mise en œuvre d'une traçabilité complète des actions sur des données, v. *infra* n°1133.

[166] C. pr. pén. art. 60-1 en enquête de flagrance qui trouve son équivalent en enquête préliminaire (art. 77-1-1) et à l'instruction (art. 99-3) : v. *infra* n°372. pour une étude détaillée de la mesure.
ROUSSEL Gildas, *Police judiciaire – Fonctionnement de la police judiciaire - § 2 - Réquisitions à distance*, Dalloz Répertoire de droit pénal et de procédure pénale, 2019.

[167] C. pr. pén. art. D15-5.

[168] *V. infra* n°373.

129. En l'état, il en résulte une ambiguïté importante sur la capacité à circonscrire les investigations numériques au sein de la procédure pénale.

§2. L'appellation « investigation numérique »

130. L'usage « d'investigation numérique » comme un tout. – L'étude des deux mots pris isolément ne parvient pas à définir correctement la notion d'investigation numérique. L'utilisation des deux mots associés dans l'expression « investigation numérique » ne permet pas, non plus, d'obtenir une définition satisfaisante, celle-ci étant perçue, à tort, comme une évidence lorsqu'elle est employée *(I)*. Il en ressort un nombre important d'ambiguïtés *(II)* sur ce qui entre dans le périmètre des investigations numériques.

I – Des définitions insatisfaisantes

131. La définition d'une agence de l'Etat. – Une définition émane de l'ANSSI[169]. Celle-ci peut être qualifiée d'officielle, car l'ANSSI est une agence de l'Etat. Dans un document pédagogique édité par cette agence dans le cadre de la labellisation *CyberEdu*[170], on trouve la « définition de l'investigation numérique *(forensics)* : ensemble des protocoles et de mesures permettant de rechercher des éléments techniques sur un conteneur de données numériques en vue de répondre à un objectif technique en respectant une procédure de préservation du conteneur ».

132. Une définition à la connotation technique trop marquée. – Il s'agit clairement d'une définition réalisée avec une vision informatique, même si le mot « mesure » pourrait, au premier abord, évoquer la notion d'acte au sens de la procédure pénale. Néanmoins, il n'est pas acceptable, juridiquement, d'affirmer que les investigations, qu'elles soient numériques comme en l'espèce ou qu'il s'agisse d'investigations en général, visent à « répondre à un objectif technique ». En procédure pénale, il y a là une

[169] ANSSI : Agence nationale de la sécurité des systèmes d'information. « L'ANSSI est l'autorité nationale en matière de sécurité et de défense des systèmes d'information. Prévention, protection, réaction, formation et labellisation de solutions et de services pour la sécurité numérique de la Nation. » *Source : « www.ssi.gouv.fr »*

[170] Labellisation de formations universitaires par l'ANSSI comme préparant les diplômés à la cybersécurité. Support de cours : « cyberedu_module_1_notions_de_base_02_2017.pdf »

totale contradiction avec le principe de licéité des preuves[171] qui s'impose aux autorités judiciaires[172], puisqu'un élément technique qui serait retrouvé par les enquêteurs, mais sans respecter le cadre légalement prévu et défini, pourrait, certes, répondre à un objectif technique, mais sans aucune utilité devant une juridiction pénale[173]. En procédure pénale, l'objectif d'une investigation est, avant toute chose, de verser au dossier des éléments respectant un cadre juridique strict[174] destinés à faire progresser le dossier[175].

133. De plus, la définition proposée par l'ANSSI est trop imprécise lorsqu'elle affirme que les investigations numériques doivent permettre la recherche « d'éléments techniques ». Il serait difficile de dire que la saisie d'une clé USB ou d'un ordinateur lors d'une perquisition est une investigation numérique[176]. Il s'agit d'une investigation classique de mise sous scellés d'un objet. Pour qu'elle devienne numérique, il faut accéder aux données et c'est donc lors de l'intervention sur les supports qu'il deviendra légitime de parler d'investigation numérique.

134. En synthèse, la définition proposée par l'ANSSI est trop restrictive car elle ne cible explicitement qu'une partie des investigations numériques. Lorsqu'il est fait référence à un « conteneur de données numériques » et à une « procédure de préservation du conteneur », on en déduit que les auteurs de cette définition pensaient aux investigations de supports numériques qui sont réalisées, selon un protocole technique précis[177], par les experts judiciaires ou par les enquêteurs spécialisés en informatique[178].

---

[171] VERGES Etienne, *Procédure pénale, op. cit.* (p.31) : Etienne VERGES explique que « le droit pénal français est dominé par le système de la liberté de la preuve ». Selon cet auteur, il est paradoxal d'affirmer que la « preuve pénale est dirigée tout à la fois par un principe de liberté et par un principe de légalité ». Parler de principe de licéité est plus juste, puisque cela respecte le principe de liberté tout en démontrant que « la recherche et la production des preuves […] doivent respecter certaines règles […] et principes […] ».

[172] Le principe de licéité ne s'appliquant pas aux autres parties, placées sous le régime de la liberté de la preuve : V. *infra* n°177. . Sur cette différence dans l'administration de la preuve, v. par ex : Crim. 7 mars 2012 – n°11-88.118 : « qu'en en tout état de cause, l'élément de preuve procuré par un particulier ne peut faire l'objet d'une annulation dès lors que n'émanant pas d'un magistrat ou d'un service d'enquête, il ne constitue pas un acte de procédure ». -

[173] Puisqu'encourant la nullité pour non-respect des règles encadrant la licéité des preuves. *Ibid.* VERGES Etienne.

[174] Des éléments techniques versés sans aucune interprétation n'auraient aucun intérêt pour le magistrat. Ceci est vrai au-delà de l'informatique. Une analyse ADN « brute » serait inexploitable dans une procédure. C'est la description du protocole technique utilisé pour procéder à l'analyse, dont le technicien déduit un pourcentage de fiabilité qui, ajouté à l'interprétation des informations, apportent des éléments concrets au juge.

[175] V. *supra* n°1.

[176] De manière classique, lorsqu'un ordinateur est découvert au domicile d'un individu, celui-ci est immédiatement placé sous scellés sans qu'aucune consultation de son contenu ne soit réalisée par les enquêteurs à ce stade. V. *infra* n°248. et 252.

[177] Utilisation d'un bloqueur en écriture, clonage des supports afin de préserver le support d'origine, etc.

[178] V. *infra* n°324.

135. Un périmètre plus vaste que les investigations sur les supports numériques. – Les investigations numériques dépassent nettement l'exploitation de supports précédemment mis sous scellés. Certaines mesures de surveillance[179] ont pour finalité de collecter des données qui, potentiellement, fournissent des informations versées au dossier et susceptibles de faire avancer la procédure[180]. Ces informations ne sont pas issues de l'exploitation d'un support, à savoir d'un « conteneur » comme cela est indiqué dans la définition.

136. La définition « grand public ». – La consultation de l'encyclopédie collaborative en ligne *Wikipedia* est représentative de la perception que le grand public peut avoir de l'investigation numérique, en énonçant que l'investigation numérique est « l'application de techniques ou de protocoles […] respectant les procédures légales et destinée à apporter des preuves numériques à la demande d'une institution [...] judiciaire[181] ».

137. Outre les nombreuses imprécisions juridiques de cette définition[182], il est intéressant de constater que cette vision des investigations numériques les attache inextricablement à des investigations judiciaires[183]. Cette restriction peut paraître surprenante pour une définition destinée à un large public, car il existe des sociétés privées qui proposent, notamment sur Internet, des prestations d'investigations numériques consistant à aider un client à se pré-constituer des preuves extraites d'un environnement informatique[184].

138. On notera également que, selon cette définition, la finalité de ces investigations est de « collecter, conserver et analyser des preuves issues de supports numériques », ce qui révèle une vision trop restrictive, à l'identique de la définition de l'ANSSI[185] : les

---

[179] V. *supra* n°68.

[180] Par ex., la géolocalisation (C. pr. pén. art. 230-32 et s.) ou les interceptions de correspondances émises par la voie des communications électroniques (C. pr. pén. art. 100 et s. et 706-95 et s.) vont conduire à exploiter des données qui sont exclusivement générées par un dispositif technique entièrement sous le contrôle des autorités judiciaires : v. *supra* n°75.

[181] « On désigne par informatique légale, investigation numérique légale ou informatique judiciaire l'application de techniques et de protocoles d'investigation numériques respectant les procédures légales et destinée à apporter des preuves numériques à la demande d'une institution de type judiciaire par réquisition, ordonnance ou jugement. On peut donc également la définir comme l'ensemble des connaissances et méthodes qui permettent de collecter, conserver et analyser des preuves issues de supports numériques en vue de les produire dans le cadre d'une action en justice. » Source : wikipedia.fr

[182] *Ibid.* V. l'emploi du mot « réquisition » ou encore l'expression « institution de type judiciaire ».

[183] *Ibid.* La définition parle d'investigation numérique légale et précise que c'est à la demande d'une institution de type judiciaire.

[184] V. *infra* n°141.

[185] V. *supra* n°134.

investigations numériques n'ont pas toutes pour finalité de fournir des preuves[186], et la formule qui veut que les preuves dont il est question soient issues de « supports numériques », sous-entend par voie de conséquence que les investigations portent toujours sur des supports comme des disques durs, des clés USB, des cédéroms, etc. Ceci est également faux[187].

139. Une vision technique prédominante. – Tout comme pour l'ANSSI, la définition proposée par *Wikipédia* est dominée par une forte connotation technique et, en tout état de cause, ne satisfait pas aux exigences d'une définition juridique. En effet, il est impossible, à partir de ces différentes sources, de cerner le périmètre de ce qui peut constituer une investigation numérique.

140. Une définition perçue comme inutile. – Les rares définitions existantes ne permettent pas de circonscrire avec suffisamment de précisions ce qu'est une investigation numérique en procédure pénale. L'absence de définition ne fait pas obstacle à l'utilisation de cette appellation[188]. Cette dernière n'est jamais définie par ceux qui l'emploient dans leurs écrits[189], aussi bien lorsque ce sont des entreprises proposant des prestations dont l'objectif est la recherche de preuves numériques, que lorsque cette expression est utilisée dans un texte juridique. A chaque fois, « investigation numérique » paraît s'imposer comme une évidence compréhensible par tous.

141. Des prestations d'investigations numériques. – Le résultat d'une recherche sur Internet[190] illustre parfaitement que l'emploi de l'appellation n'est assorti d'aucune définition. En effet, la majorité des résultats renvoie à des sites de professionnels qui proposent des investigations numériques privées[191]. La consultation de ces sites montre

---

[186] V. *supra* n°111.
[187] V. *supra* n°135.
[188] V. par ex. dans la presse généraliste : NASI Margherita, *Matthieu, le hackeur qui plaide pour la sécurité informatique,* Le Monde Eco et entreprise, 18 septembre 2012 : « […] start-up de sécurité informatique offrant services et produits d'investigation numérique permettant aux entreprises d'analyser la sécurité de leurs produits ou de leurs systèmes ».
[189] MEDDAH Hassan, *Cyber cherche experts désespérément,* L'usine Nouvelle n°3642, 16 janvier 2020 : « Les profils les plus recherchés concernent les postes techniques : spécialiste en investigation numérique, architecte de systèmes, analyste en cybermenaces... ». Pour l'auteur, le profil des « spécialistes en investigation numérique » est tout aussi facile à cerner que les deux autres fonctions citées, qui correspondent à des métiers informatiques parfaitement identifiés.
[190] www.google.fr : recherche sur « investigation numérique ».
[191] www.technapol.fr/investigation-numerique
www.celog.fr/metiers-expertises/investigation-numerique
www.tracip.fr
www.nolimitsecu.fr/category/investigation-numerique, etc.

que ces sociétés n'éprouvent pas le besoin de définir ce qu'est une investigation numérique. Elles décrivent directement des cas pratiques, au travers desquels elles font ressortir la nécessité de procéder à ce qu'elles qualifient d'investigations numériques, auxquelles elles associent évidemment les prestations qu'elles proposent[192]. Par là-même, elles considèrent que l'expression « investigation numérique » est intuitivement compréhensible par tous. Il s'agit en conséquence d'une sorte de définition par le contenu des prestations proposées par ces sociétés sous l'appellation d'investigation numérique.

142. Des contradictions dans les définitions tacites. – Ces structures étant des sociétés privées dénuées de toute mission judiciaire[193], leur vision de ce qu'est une investigation numérique contredit la définition de *Wikipédia* qui l'associait à des recherches judiciaires[194]. En effet, les prestations proposées par ces sociétés commerciales se positionnent au niveau de la pré-constitution des preuves, à savoir en amont d'une éventuelle procédure judiciaire. Il en ressort un besoin indispensable de clarifier précisément ce que sont les investigations numériques qui sont le fruit de la dématérialisation de certains actes d'enquête. En effet, au sein de la procédure pénale, aucune définition usuelle ne peut convenir pour identifier avec précision quelles sont les mesures entrant dans cette catégorie.

143. L'utilisation « d'investigation numérique » dans la doctrine juridique. – L'emploi de l'appellation par des sociétés privées montre qu'elle est spontanément perçue comme intelligible pour tout un chacun. Pour autant, aucune clarification définitivement satisfaisante n'est apportée. Dans les écrits juridiques, l'expression est peu utilisée mais elle est également perçue comme une évidence lorsqu'elle l'est. Tout d'abord, on ne trouve aucun emploi « d'investigation numérique » dans les Codes. Ensuite, l'appellation est également peu utilisée par la doctrine ainsi que dans les décisions des juridictions.

144. Dans la doctrine, il est rare qu'il y soit explicitement fait référence. Un usage exceptionnel est présent en droit civil. Il concerne les pouvoirs de contrôle et de sanction de la CNIL[195]. On constate immédiatement que, pour l'auteur, la compréhension de ce

[192] Celog : « La copie de disque dur – L'analyse de disque dur – Analyse d'appareils mobiles »
TRACIP : « Sécurisation et collecte de preuves – Recherche et analyse »

[193] Sauf si, en leur sein, l'un de leur technicien est inscrit sur une liste d'expert près une Cour d'appel ou sur la liste nationale (v. *infra* n°301. et s.), et que celui-ci soit commis ou réquisitionné.

[194] V. *supra* n°137.

[195] DAUTIEU Thomas, *La Commission Nationale de l'Informatique et des Libertés Saisine par les particuliers – Pouvoirs de contrôle et de sanction,* JurisClasseur Communication, Fasc. 4733 : « Investigations numériques – Les éléments utiles peuvent ne pas être communiqués directement par

que sont des investigations numériques ne soulève aucune difficulté : il s'agit de rechercher des éléments numériques au sein de l'infrastructure informatique présente dans les locaux qui sont la cible du contrôle de la CNIL. Ceci rejoint, dans les grandes lignes, les définitions techniques proposées par l'ANSSI[196] ou par *Wikipedia*[197]. Les propos de l'auteur nous renvoient également vers une entité nommée l'AFSIN[198], dont le site Internet de cette dernière[199] ne comporte pas, non plus, de définition à proprement parler.

145. En matière pénale, l'expression « investigation numérique » est également peu présente. Une seule jurisprudence de la Cour de Cassation la comportant est retrouvée[200] : elle ne présente aucun intérêt, si ce n'est d'en retenir que les magistrats n'éprouvent également pas le besoin de préciser ce dont il s'agit. Quelques jurisprudences de Cours d'appel[201] n'apportent rien car elles présentent la même caractéristique que celle de la chambre criminelle.

146. Dans la doctrine pénaliste, chaque fois que l'expression est employée, elle paraît toute aussi évidente à comprendre pour l'auteur[202], même si les utilisations sont peu nombreuses. Néanmoins, la référence aux investigations numériques tend actuellement à augmenter car de plus en plus d'auteurs s'intéressent à la cybercriminalité[203] ou à ce que l'on nomme le droit de l'informatique ou Technologies de l'Information et de la Communication.

---

le responsable des lieux soit parce qu'il ignore leur existence (par exemple, dans le cas d'un fichier créé par un des salariés à son initiative) soit parce qu'il ne révèle pas leur existence aux membres de la délégation. Pour pallier à ces difficultés, les agents de la commission peuvent utiliser, lors des contrôles sur place qu'ils mènent, des moyens informatiques de recherche – voire de récupération – de données. Sur ce point, on peut mentionner que la CNIL est membre de l'Association francophone des spécialistes de l'investigation numérique (AFSIN). L'ensemble des investigations numériques effectuées par les membres de la délégation sont portées à la connaissance du responsable des lieux, sont faites en sa présence ou en présence de son représentant et actées, ainsi que leurs résultats, dans le procès-verbal rédigé à l'issue du contrôle. »

[196] V. *supra* n°131.

[197] V. *supra* n°136.

[198] « L'AFSIN a pour vocation d'établir un dialogue constant entre les différents participants, techniciens, juristes, à l'opération d'investigation numérique. » Extrait des statuts de l'association, art. 2.

[199] https://new.afsin.org

[200] Crim. 28 mars 2012 n°11-83.012 : « […] la réquisition au technicien d'investigations numériques qualifié dans le domaine des infractions liées aux nouvelles technologies de l'information et de la communication ayant motivée la rédaction du rapport d'examen technique du 6 octobre 2008 […] » et « […] la réquisition au technicien d'investigations numériques du 29 octobre 2008 […] ».

[201] V. CA Paris 5 oct. 2016 n°14/25251 – CA Lyon 1 déc. 2010 n°08/01170.

[202] V. par ex. QUEMENER Myriam, *Perquisitions et saisies de données informatiques dans le cadre de l'état d'urgence*, Dalloz IP/IT, 2016, p. 499 : « En effet, à l'heure où les investigations numériques sont devenues incontournables dans la plupart des enquêtes et en particulier lors des […], il était problématique de ne pas pouvoir pratiquer de saisies informatiques particulièrement dans le cadre de l'état d'urgence. »

[203] V. *supra* n°32. Par ex. Myriam QUEMENER *(ibid.)* évoque les « […] investigations qui portent, désormais, sur l'exploitation de données récupérées sur tous les supports numériques. »

147. Conclusion du sous-paragraphe I : des définitions insatisfaisantes. – Aucune définition probante ne ressort de l'emploi de la notion d'investigation numérique lorsqu'elle est utilisée, aussi bien par des professionnels de l'informatique qu'au sein de la doctrine juridique.

Pourtant, de nombreuses imprécisions ne sont pas acceptables car elles font naître des ambiguïtés sur ce qui peut être réellement considéré comme une investigation numérique.

II – Des ambiguïtés bloquantes

148. L'ambiguïté autour de l'environnement numérique de la cible de l'investigation. – Certes, le cas, où les enquêteurs[204] utilisent des outils numériques[205] pour investiguer dans l'environnement, lui-même numérique, de leur cible, ne soulève aucune difficulté : ils procèdent à des investigations numériques. Néanmoins, de nombreuses situations ne sont pas aussi claires. Par exemple, une première question se pose avec des investigations pour lesquelles les enquêteurs utilisent des outils numériques, mais sans investiguer dans l'environnement numérique de la cible[206]. S'agit-il d'investigations numériques ? La réponse est affirmative puisque les enquêteurs génèrent des données[207] lors de l'exécution de l'acte d'enquête en question[208].

149. L'ambiguïté issue de la confusion entre numérique et électronique. – Cette réponse appelle une nouvelle question, plus prégnante. Comme expliqué précédemment[209], les écrits juridiques ont tendance à confondre « digital[210] » et « électronique », générant par là-même une grande confusion sur les rapports entre les investigations numériques, les outils utilisés, et leur utilisation au sein des enquêtes[211].

---

[204] Ou, éventuellement, un expert judiciaire qui serait commis ou réquisitionné pour une analyse de support numérique précédemment saisi : voir *infra* n°300.

[205] Logiciels d'investigation, matériels tels que bloqueur de disque dur, voire, tout simplement, un ordinateur relié à l'environnement informatique du lieu objet d'une perquisition : v. *infra* n°257.

[206] Par ex : la géolocalisation physique d'un véhicule au travers d'un dispositif implanté par les enquêteurs. C. pr. pén. art. 230-32 et s. Pour une étude détaillée de la mesure, v. *infra* n°489.

[207] V. la définition d'investigation : *supra* n°111. Dans le cas de l'exemple précédent (géolocalisation), il s'agit de rechercher une preuve de la présence d'un individu à un endroit donné et à un instant « t ».

[208] V. la définition de numérique : *supra* n°115. Toujours avec l'exemple de la géolocalisation, et suivant le type de dispositif utilisé, il s'agira d'un fichier listant des coordonnées GPS horodatées.

[209] V. *supra* n°115.

[210] *Ibid.* Synonyme de numérique.

[211] V. LESCLOUS Vincent, *Chronique – Un an de droit de la garde à vue (1er juin 2010 - 1er juin 2011),* JurisClasseur Droit pénal n°9 Septembre 2011, chron. 7 : « On ne peut à cet égard que souhaiter le développement des moyens de police scientifique, de vidéoprotection ou d'investigation numérique destinés au recueil de preuves objectives. » L'extraction des données d'un système de vidéoprotection fait partie des investigations numériques et les investigations numériques peuvent être incluses dans les moyens de police scientifique.

150. Or, dans le cas, notamment, de la sonorisation ou de la « fixation d'images de certains lieux ou véhicules[212] », peut-on considérer, en fonction des dispositifs techniques utilisés, qu'il s'agit systématiquement d'investigations numériques ? Si les enquêteurs décident d'écouter ou de visualiser en temps réel un lieu ou un véhicule, sans enregistrer, afin de pouvoir intervenir à un moment opportun, aucune donnée n'est produite par cet acte et il ne s'agit donc pas d'une investigation numérique.

151. De même, si un vieux caméscope à cassette est utilisé pour filmer l'intérieur d'un local ou, même si avec un caméscope numérique, les enquêteurs se contentent de visualiser le contenu en le projetant sur un écran sans en extraire les fichiers vidéos, on ne peut pas parler d'investigation numérique puisqu'aucun fichier numérique (en l'occurrence, une vidéo) ne sera versé à la procédure[213].

152. Le raisonnement est identique avec la géolocalisation[214] dans le cas où les enquêteurs se limiteraient à utiliser un dispositif grâce auquel ils suivent, par exemple, un véhicule en temps réel. Avec ce type d'équipement, aucune donnée de localisation n'est enregistrée. L'appareil se limite à indiquer une direction et une distance. On se trouve alors dans une situation de filature techniquement assistée, mais pas dans le cadre d'une investigation numérique.

153. L'ambiguïté des fichiers de police. – Inversement, avec la multiplication des « fichiers judiciaires et administratifs », autrement dit les traitements de données à caractère personnel mis en place par l'Etat ces dernières années[215], il est légitime de se demander si la consultation de ces fichiers correspond à la définition des investigations numériques. Ce questionnement n'est pas négligeable tant ces bases de données ont pris une importance grandissante, notamment à la suite aux attentats ayant frappés la France depuis 2015[216].

---

[212] C. pr. pén. art. 706-96 et s. Pour une étude détaillée de la mesure, v. *infra* n°454.
[213] Sur la distinction entre vidéosurveillance et vidéoprotection (sur la vidéoprotection v. *infra* n°451.), v. Wolters Kluwer, *Chapitre 3 Règles spécifiques à l'installation des systèmes de vidéoprotection et de vidéosurveillance,* Le Lamy droit du numérique (Guide), 2019.
[214] V. *infra* n°486.
[215] V. *infra* n°603.
[216] RASCHEL Evan, *Sécurité intérieure – La sécurité intérieure et la lutte contre le terrorisme entre cadence et décadence : commentaire de la loi n°2017-1510 du 30 octobre 2017*, LexisNexis, Droit pénal n°12, décembre 2017, étude n°23.

154. Certes, certains traitements sont anciens tels que les fichiers d'antécédents de la Police Nationale et de la Gendarmerie, qui existaient depuis longtemps même s'ils n'ont été officialisés qu'en 2001[217] (JUDEX et STIC), puis fusionnés en 2015 dans le TAJ[218]. D'autres fleurissent cependant au gré des différentes lois, tout particulièrement en matière de renseignement ou de lutte contre le terrorisme (fichier judiciaire national automatisé des auteurs d'infractions terroristes[219], traitement automatisé de données à caractère personnel dénommé « Enquêtes administratives liées à la sécurité publique »[220], traitement de données à caractère personnel dénommé « Gestion de l'information et prévention des atteintes à la sécurité publique »[221], etc).

155. Une véritable investigation numérique. – Les définitions des deux mots pris isolément[222] (« investigation » et « numérique ») ne laissent aucune ambiguïté quant à une réponse positive, puisque la consultation d'un traitement de données aussi sensible et particulier, constitue à n'en pas douter une « recherche attentive[223] » et que, d'autre part, les informations extraites de ces fichiers sont intrinsèquement « numériques » puisqu'issues d'un traitement informatique.

156. Conclusion de la section 1 : l'erreur d'une définition perçue comme évidente. – La doctrine n'éprouve pas le besoin de définir la notion « d'investigation numérique », alors que l'utilisation qui en est faite montre que les auteurs ne se réfèrent pas à des actions identiques. C'est clairement le mot « numérique » qui est la source de l'instabilité. Cette dernière découle principalement d'une confusion qui est faite avec le mot « électronique ». En procédure pénale, il est impossible, en l'état actuel, de savoir si une investigation numérique est une investigation reposant sur des outils technologiques, ou si elle concerne exclusivement des recherches dans un environnement informatique. Pour ajouter de la confusion, les définitions des mots « investigation » et « numérique » démontrent que la consultation et l'extraction de données depuis des traitements à caractère personnel sont des investigations numériques.

---

[217] 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 (STIC).
[218] Décret n°2013-1268 du 27 décembre 2013 portant modification du décret n°2012-652 du 4 mai 2012 relatif au traitement d'antécédents judiciaires *(entrée en vigueur différée au 31 décembre 2015).*
[219] C. pr. pén. art. 706-25-3 et suiv.
[220] C. pr. pén. art. R236-1 et suiv.
[221] C. sec. int. art. R236-21 et suiv.
[222] V. *supra* n°109. et s.
[223] V. *supra* n°111.

Section 2. L'erreur d'une définition par la preuve numérique

157. Un lien imparfait. – Afin de pallier l'absence de définition précise de « l'investigation numérique », il est tentant d'établir une sorte de lien parfait entre cette appellation et la « preuve numérique[224] ». Ce lien reviendrait à permettre la définition d'une notion par l'autre.

Une étude de la définition de la « preuve numérique » *(§1)* montre que cette notion n'est pas plus stable que celle « d'investigation numérique ». De plus, même si les deux notions ont une importante intersection, elles ne se superposent pas parfaitement *(§2)*.

§1. L'instabilité de la notion de preuve numérique

158. La vaste notion de preuve. – De même que « l'investigation numérique » est avant tout une investigation[225], la « preuve numérique » est un sous-ensemble de la preuve. Or, la doctrine explique que « la preuve peut se définir comme une démonstration aux fins de persuader de l'exactitude d'un fait allégué en vue de faire prévaloir un droit[226] », ce qui découle de l'article 1353 du Code civil[227] qui dispose que « celui qui réclame l'exécution d'une obligation doit la prouver ».

159. Même si l'appréhension de la preuve par le Code civil trouve rapidement ses limites en procédure pénale[228], ceci donne une définition générale de la preuve par son objectif : démontrer quelque chose. En matière pénale « la preuve consiste non seulement à démontrer l'existence d'un fait, mais encore son imputation à une personne ainsi que, la plupart du temps, l'intention que celle-ci avait de commettre un tel fait[229] ».

Dans le cadre de ce triptyque « fait-imputation-intention[230] », on est bien en présence d'une définition par l'objet de la preuve pénale, dont la finalité consiste à corroborer les trois éléments[231].

---

[224] V. *supra* n°114. On déduit de certaines définitions et des écrits de certains auteurs, que l'investigation numérique aurait pour unique finalité de chercher des preuves numériques. D'où la supposition d'un lien parfait entre les deux notions qui permettrait de définir l'une par l'autre.

[225] V. *supra* n°1. et n°85.

[226] PRADEL Jean, *Procédure pénale - Op. cit* p.31

[227] Ancien article 1315 avant la réforme du droit des contrats par l'ordonnance n°2016-131 du 10 février 2016 (*op. cit.* p.12).

[228] V. par ex. C. pr. pén., art. 427 qui dispose que la force probante des preuves est laissée à la libre appréciation du juge et n'est donc pas fixée à l'avance par la loi, contrairement au Droit civil ou les moyens de preuve sont souvent encadrés, comme lorsqu'un acte authentique (C. civ. art. 1369 et s.) est exigé.

[229] V. BUISSON Jacques, *Preuve*, Répertoire de droit pénal et de procédure pénale, Dalloz, al. n°1.

[230] POUYANNE Julia, *L'auteur moral de l'infraction*, Presses universitaires d'Aix-Marseille, 2003.

[231] Ou l'un des trois puisqu'une preuve peut prouver, par exemple, uniquement l'élément intentionnel d'un individu, alors que ce sont d'autres preuves, différentes, qui s'intéressent aux faits.

160. La notion de preuve parfaitement définie. – Même si le concept de preuve n'est pas explicitement théorisé dans le Code de procédure pénale[232], cette notion est parfaitement compréhensible dans le vocabulaire juridique[233], notamment grâce au cadre qui entoure l'administration de la preuve[234].

161. L'incertitude du mot « numérique ». – Néanmoins, lorsqu'on s'intéresse à la notion de « preuve numérique », on retrouve les mêmes sources d'instabilité qu'avec « investigation numérique », en raison du mot « numérique ». C'est, soit une vision trop technique qui se dégage, soit une notion perçue comme évidente par ceux qui l'emploient[235] .

162. De même, il existe une confusion toute aussi importante avec les mots « numérique » et « électronique » lorsqu'ils sont associés à « preuve », y compris dans des textes récents[236] . Le Conseil Justice et affaires intérieures parle à de nombreuses reprises de « preuve électronique » dans un emploi totalement à contre-sens. Il est évident que l'appellation « preuve numérique » aurait été mieux adaptée puisque c'est clairement à une preuve dématérialisée que se réfère le Conseil et en aucun cas à une preuve qui serait extraite de composants électroniques[237]. Ce contre-sens se retrouve dans les lignes directrices adoptées par le Comité des Ministres du Conseil de l'Europe[238]. La définition qui est énoncée au cœur de ce texte démontre qu'il s'agit d'une preuve numérique et non d'une preuve électronique puisqu'elle « découle de données » ou produites par un environnement informatique, donc numérique par essence.

---

[232] V. *supra* n°87.

[233] CORNU Gérard, *Vocabulaire juridique, op. cit.* (p.7). Preuve : « démonstration de l'existence d'un fait ou d'un acte dans les formes admises et requises par la loi ».

[234] V. C. pr. pén. art. 427 qui pose le principe de liberté de la preuve, qui est placé dans un paragraphe intitulé « De l'administration de la preuve ». V. également PRADEL Jean, *Procédure pénale, op. cit.* (p.31) sur « la légalité dans l'administration de la preuve », p.368 et s.

[235] V. *supra* n°140.

[236] V. le compte-rendu de la réunion des 8 et 9 juin 2017 du Conseil Justice et affaires intérieures, sur la partie « Justice pénale dans le cyberespace » ou encore le compte-rendu de la réunion des 12 et 13 octobre 2017 du même conseil
Source : www.consilium.europa.eu/fr/meetings/jha/2017/06/08-09/

[237] V. *supra* n°116. Le mot « électronique » est beaucoup plus restrictif que le mot numérique puisqu'il ne vise que des preuves qui seraient extraites d'un disque dur ou d'une clé USB par exemples (à savoir des objets à base de composants électroniques). Les données qui seraient obtenus depuis un traitement de données à caractère personnel au visa de l'article art. 60-1 du C. pr pén.(V. *supra* n°126.) ne seraient pas incluses, puisqu'extraites d'un environnement de type *Cloud* (V. *infra* n°221.) et donc totalement détachées des composants électroniques qui hébergent la donnée à un instant « t ».

[238] V. les lignes directrices du Comité des Ministres du Conseil de l'Europe sur les preuves électroniques dans les procédures civiles et administratives adoptées par le Comité des Ministres le 30 janvier 2019
Source : https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=0900001680902dc9

163. La vision purement technique. – Les Hommes de l'art qui utilisent l'expression « preuve numérique » ont une vision trop « technique » de celle-ci[239]. Il est aisé de comprendre que celle-ci provient de l'orientation très « civiliste » des recherches d'informations numériques que la majorité des experts judiciaires en informatique[240] ont à réaliser. En effet, très souvent, les experts interviennent en appui à un huissier de justice dans le cadre d'une « ordonnance 145[241] », voire même en amont de toute procédure pour une pré-constitution de preuve qu'une personne (physique ou morale) souhaite réaliser[242].

164. Dans ce cas, la collecte des informations numériques se fait de manière unilatérale et lorsqu'ultérieurement une procédure s'engage au fond[243], la partie à laquelle sont opposés ces éléments précédemment recueillis, va souvent contester leur véracité. Ainsi, la vision informatique des experts positionne l'intégralité du problème de la force de la preuve sur les conditions techniques dans lesquelles sont collectées et analysées ces données[244].

165. L'erreur de la vision d'une technique prépondérante sur le juge. – Il s'agit là d'une vision erronée de la répartition des rôles : seul le juge est compétent pour déterminer si une preuve est recevable, et tout particulièrement en procédure pénale ou l'encadrement du recueil des preuves est strict. Une investigation numérique peut prendre toutes les précautions techniques qui soient possibles, si elle est exécutée en violation du cadre légal qui la prévoit, l'annulation de son résultat paraît évidente[245].

166. L'intégrité et l'authenticité des informations numériques qui sont mises en évidence dans un rapport par un expert font intégralement partie de la mission technique qui lui est confiée. Il lui incombe d'énoncer les éventuelles incertitudes qui entoureraient

---

[239] MIGAYRON Serge, *Informatique – Pratique contentieuse. De l'information numérique à la preuve,* LexisNexis, Communication Commerce Electronique n°4, avril 2017.

[240] V. *infra* n°301. .

[241] Expression en référence à l'art. 145 du C. pr. civ. art. qui prévoit que des mesures peuvent être ordonnées « sur requête », c'est-à-dire de manière non contradictoire. L'objectif est ici bien sûr de se prémunir d'un éventuel dépérissement de preuves qui s'avèreraient nécessaires à la solution d'un litige.

[242] Par ex. conflit entre un employeur et un salarié, divorce, etc. Dans toutes ces situations, la problématique consiste à recueillir des informations numériques dans un environnement informatique, selon des modalités qui permettront ultérieurement de les opposer à un tiers.
Sur un constat d'huissier réalisé en amont d'une procédure pénale, v. Crim. 8 janv. 2019 n°18-80.748.

[243] L'ordonnance sur requête délivrée au visa de l'art. 145 du C. pr. civ. n'a, en aucun cas, vocation à trancher un contentieux, qui doit faire l'objet d'une procédure au fond.

[244] *Ibid.* MIGAYRON Serge : « Les deux critères essentiels qui permettent de qualifier une information numérique de preuve sont les critères d'intégrité et d'authenticité ». Il est clair que pour Serge MIGAYRON, la complétude de la preuve numérique se joue exclusivement au niveau technique.

[245] V. *supra* n°132.
Sur le régime des nullités, v. *infra* n°856.

une information qu'il communique dans son rapport afin que le magistrat puisse la considérer comme il se doit. Malheureusement, l'expert judiciaire est parfois mal à l'aise avec la présentation de ses travaux[246], tout particulièrement en matière pénale[247].

167. L'évidence de la définition de preuve numérique dans la doctrine. – Chez les auteurs juridiques, la notion de « preuve numérique » a en commun avec celle « d'investigation numérique » d'être mal ou peu définie[248], et d'être perçue comme naturellement compréhensible par tous. On ne trouve aucun auteur qui se soit investi dans une véritable définition, et il y a peu de travaux scientifiques qui ont été réalisés sur ce sujet[249]. En revanche, malgré cette absence de définition, l'appellation « preuve numérique » commence à entrer dans le vocabulaire courant des juristes et est plus employée « qu'investigation numérique[250] ».

168. Les auteurs qui travaillent sur le droit du numérique manipulent donc cette notion sans se poser de question, à l'instar de Myriam QUEMENER[251]. De même, Christiane FERAL SCHUHL ne définit pas à proprement parler la « preuve numérique », mais on déduit de ses propos que c'est la preuve recueillie dans un environnement numérique[252], ce qui est implicitement corroboré par Frédérique CHOPIN qui parle à plusieurs reprises de preuve numérique « […] dans le contexte des communications électroniques[253] ».

169. L'incertitude révélée par des contradictions. – Pour autant, l'apparente évidence qui se dégage de l'utilisation faite de « preuve numérique » par ces auteurs est mise à mal par des contradictions qui ressortent de leurs propres propos.

170. Pour Myriam QUEMENER les preuves numériques sont issues de « l'exploitation de données récupérées sur tous les supports numériques ». Est-ce à dire que les

[246] SAVART Michel (Directeur du laboratoire de police scientifique de Lyon), *l'expertise scientifique en matière pénale,* Dalloz AJ pénal 2006 p72 : « les scientifiques sont habitués à présenter leurs résultats issus de méthodes souvent complexes, en utilisant des outils de communication […] qui ne sont pas d'usage courant dans les salles d'audience françaises. »
[247] V. *infra* n°303.
[248] V. *supra* n°130.
[249] Deux thèses sur ce thème : HENNEQUIN Shirley, *La preuve numérique dans le procès pénal*, soutenue en 2011 à Aix-Marseille et FARGEAUD Pierre, *La preuve informatique en droit français : les aspects juridiques de l'inforensique,* soutenue en 2007 à Limoges.
[250] V. *supra* n°104.
[251] QUEMENER Myriam, *Les spécificités juridiques de la preuve numérique*, AJ Pénal 2014 p.63.
[252] FERAL SCHUHL Christiane, *La collecte de la preuve en matière pénale*, AJ Pénal 2009 p.115.
[253] CHOPIN Frédérique, *Modes de preuve dans le contexte des communications électroniques*, Répertoire de droit pénal et de procédure pénale, Dalloz.

informations issues de données extraites de traitements de données[254] (judiciaires ou mis en œuvre par une structure privée) ne constitueraient pas une preuve numérique ?

171. Christiane FERAL SCHUHL, quant à elle, cible son analyse sur « les preuves [qui] peuvent s'avérer difficiles à rapporter dans l'environnement numérique, d'autant que les délinquants peuvent aisément les détruire ou les déplacer ». Elle semble penser que seules les données appartenant au délinquant peuvent déboucher sur des preuves numériques. Pourtant, les mesures de surveillance génèrent des données susceptibles de produire des preuves[255], numériques par essence, et qui ne sont pas la « propriété » du délinquant[256].

172. Cédric MICHALSKI, pour sa part, parle de « dématérialisation des preuves[257] » ce qui est différent de la preuve numérique. En effet, des documents « papier » qui seraient retrouvés au cours d'une perquisition et qui seraient scannés pour être envoyés, par exemple, à une juridiction géographiquement distante, deviennent dématérialisés sans qu'ils constituent pour autant une preuve obtenue dans un environnement numérique.

173. L'impossibilité de définir une notion par une notion incertaine. – Les mêmes ambiguïtés et les mêmes questionnements unissent les notions de preuve numérique d'investigation numérique[258]. Dans ces conditions, considérer que l'investigation numérique peut être définie par son objet, qui serait de collecter des preuves numériques, est une erreur[259]. Cette notion soulève, elle-même, bon nombre d'interrogations sur ce qu'elle regroupe exactement, et ne peut donc pas servir à définir l'investigation numérique.

---

[254] En application de l'art. 60-1 du C. pr. pén. en enquête de flagrance (qui trouve son équivalent en enquête de flagrance, art. 77-1-1 et à l'instruction, art. 99-3) : v. *infra* n°372. pour une étude détaillée de la mesure.
[255] V. *supra* n°68.
[256] *Ibid.*
[257] MICHALSKI Cédric, *La recherche et la saisie des preuves électroniques*. *Op. cit.* p.35
[258] V. *supra* n°156.
[259] V. *supra* n°136. : *Wikipedia* énonce que les investigations numériques sont « destinées à apporter des preuves numériques ».
LESCLOUS Vincent (*op. cit* p.35) affirme que les « investigations numériques sont destinées au recueil de preuves objectives ».

§2. L'impossible assimilation de la preuve numérique et de l'investigation numérique

174. Deux notions différentes. – Outre les incertitudes qui entourent les deux notions de « preuve numérique » et « d'investigation numérique », elles doivent être distinguées car elles ne se recouvrent pas totalement : elles définissent deux ensembles, certes ayant une grande intersection, mais malgré tout disjoints.

175. L'intersection des deux notions. – L'intersection des deux notions est intuitivement évidente. Chaque fois qu'une investigation numérique débouche sur une preuve dont la qualification de numérique ne soulève pas de difficulté[260], le lien entre les deux notions est parfait.

176. Les différences des deux notions. – Même si la majorité des cas où les autorités judiciaires ont recours aux investigations numériques se trouvent dans l'intersection entre les deux notions, celles-ci ne se recouvrent pas car « l'investigation numérique » est plus vaste que la notion de « preuve numérique », de même que toutes les preuves numériques ne sont pas forcément issues d'investigations numériques.

177. Les preuves apportées par les parties. – En effet, seules les autorités judiciaires diligentent, dans le respect de la procédure, des investigations, et donc des investigations numériques. Or, cela ne fait pas obstacle au fait que les autres parties (suspect, mis en examen, partie civile) peuvent prouver leurs dires par tout moyen, puisque le principe de licéité des preuves[261] s'épuise considérablement dans son application aux parties autres que la puissance publique[262]. C'est le cas, notamment, au travers de la production de documents informatiques tels que des courriels ou des fichiers[263] qui, s'ils participent à convaincre le juge, deviennent alors des preuves numériques. Dans la continuité, même de simples témoins peuvent fournir, lors de leur audition, des éléments (ordinateurs spontanément remis à la Police, cartes mémoire d'appareils photos, etc) également

[260] V. *infra* n°169.
[261] V. *supra* n°132. sur la différence entre licéité et légalité des preuves.
[262] LEPAGE Agathe, *Tel est pris qui croyait prendre… mais est sauvé par le principe de loyauté de la preuve*, Communication Commerce Electronique n°11 novembre 2016 : « L'enjeu tient au fait qu'en droit pénal le principe de la loyauté de la preuve […] se montre autant accommodant à l'endroit des parties privées que rigoureux à l'égard des autorités publiques. »
[263] Ex. : des lettres, des documents comptables, des journaux de connexion, des historiques de caches internet, etc.

susceptibles de devenir de telles preuves, sans pour autant être issus d'investigations numériques.

178. L'investigation plus vaste que la preuve. – Inversement, les investigations numériques ne débouchent pas systématiquement sur une preuve. Dans leur recherche des auteurs des infractions, les enquêteurs explorent souvent de nombreuses « pistes », parmi lesquelles un certain nombre ne débouche sur rien, pas même un indice[264].

179. C'est d'ailleurs dans la distinction que certains auteurs[265] opèrent entre « preuve », « indice », « charge » ou encore « présomption », que l'on trouve le point de divergence le plus important entre « investigation numérique » et « preuve numérique ».

180. L'indice, dans son sens premier, est un « signe qui révèle l'existence d'une chose[266] ». Intuitivement, on positionne donc l'indice comme un élément moins fort que la preuve ou, autrement formulé, qui n'est pas encore une preuve (ce qui sous-entend qu'un indice peut ne jamais devenir une preuve, notamment s'il est démontré qu'il est faux, mal interprété ou utilisé à mauvais escient). D'ailleurs, on notera que le Code de procédure pénale emploie notamment ce mot dans les articles 53 et 54 relatifs aux enquêtes de flagrance, à savoir à un stade de la procédure très proche de la commission ou de la découverte de faits répréhensibles, et où tout doit donc être fait pour préserver et collecter ces « indices », mais surtout à un moment où la vérité judiciaire est encore loin d'être établie.

181. Le mot « présomption », quant à lui, est le plus souvent associé à la « présomption d'innocence ». Mais, il est également employé à trois reprises dans le Code de procédure pénale[267], sous sa signification première : « opinion fondée seulement sur des indices, des apparences, des commencements de preuves[268] ». On en déduit que la présomption n'est pas encore aussi forte que l'intime conviction du juge telle que décrite à l'article 427 du Code de procédure pénale[269], mais elle se réfère bien à une « opinion », qui repose sur des indices. Aussi, c'est par abus de langage que le terme « présomption » est parfois

[264] Ces investigations réalisées pour éliminer ces pistes infructueuses, ne se recoupent donc pas avec la notion de preuve.
[265] Par ex. BUISSON Jacques, *Preuve* (*op. cit.*, p. 35) : « Ces modes de preuve permettent de recueillir des éléments de preuve qui, dénommés « indices » pendant l'enquête ou l'instruction peuvent devenir des « charges » dans l'exercice de poursuite devant le juge de jugement et des « preuves », une fois prononcée la culpabilité par la juridiction de jugement. »
[266] Dictionnaire Littré.
[267] Art. 28-2, 705 et 706-11.
[268] Dictionnaire Littré.
[269] C. pr. pén. art. 427, *op. cit.* : « 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. […] »

utilisé comme un synonyme d'indice. D'ailleurs, lorsque les articles 705 et 706-11 du Code de procédure pénale, parlent, au sujet d'infractions, de « présomptions caractérisées », c'est-à-dire une présomption plus forte qu'un simple indice, l'assimilation au mot « preuve » paraît alors évidente.

182. L'expression « les charges » est employée à plusieurs reprises dans le Code de procédure pénale, notamment dans le titre III relatif aux juridictions d'instruction : « charges constitutives d'infraction[270] », « charges suffisantes[271] », « charges recueillies apparaissent suffisantes[272] ». Cet emploi fait naître une ambiguïté avec la définition du dictionnaire Littré qui les définit comme des « faits qui militent en faveur de la culpabilité ». En effet, on comprend que le Code de procédure pénale fait du mot « charge » un quasi-synonyme de « preuve », puisqu'il s'agit d'un élément retenu contre le mis en examen, tandis que le Littré qualifie les charges de « faits », ce qui fait plutôt penser que les charges sont démontrées par des preuves.

183. *A contrario*, d'autres auteurs ne font guère de différence entre ces termes : « on ne fait, à tous les stades de la procédure, que rechercher, rassembler et évaluer des preuves qui ne se distinguent que par le fait qu'on ne demande pas le même degré de vraisemblance ou de certitude à tous les échelons de la procédure. Cela se traduit par la terminologie employée[273] ». Cette identité des différents termes trouve sa source, pour une partie de la doctrine, dans l'importance des « procédés modernes d'investigations[274] » qui « ont bouleversé le procès pénal[275] ». En effet, les techniques modernes[276] ont « abouti à une sorte d'hypertrophie de la catégorie des indices[277] » rendant la distinction entre ces différents termes inadaptée. Globalement, les auteurs s'intéressant au droit du numérique ne font pas, non plus, cette différence terminologique. C'est notamment le cas avec Myriam QUEMENER qui considère clairement les expressions « preuves numériques » et « indices numériques » comme synonymes[278].

---

[270] C. pr. pén. art. 176.
[271] C. pr. pén. art. 177.
[272] C. pr. pén. art. 182.
[273] RASSAT Marie-Laure*, Procédure pénale,* 2ème édition, Ellipses, p.239
[274] AMBROISE-CASTEROT Coralie et BONFILS Philippe, *Procédure pénale,* puf Thémis droit, 2ème édition, p. 184.
[275] *Ibid.*
[276] Analyse sanguine, génétique.
[277] *Ibid.*
[278] V. *supra* n°168. : Myriam QUEMENER, dans l'ensemble de ses publications, emploie indifféremment les termes « preuve numérique » et « indice numérique ».

184. Des termes différents couverts par la notion d'investigation numérique. – Ce débat sémantique est une parfaite illustration de la différence qui existe entre « investigation » et « preuve » numérique. En effet, l'investigation numérique est plus vaste, voire en amont, de la notion de preuve, d'indice ou de charge. Elle a pour objet de fournir au sein de la procédure pénale, des éléments destinés à la faire avancer et, *in fine*, à la clore[279].

185. Des investigations dont la finalité n'est pas la recherche de preuve. – Toutes les investigations n'ont pas pour finalité de rassembler des preuves. Il en est ainsi dans le cas de la découverte d'un cadavre[280], de la recherche d'une personne en fuite[281] ou disparue de manière inquiétante[282].

186. Il convient de rappeler qu'une investigation a pour objectif de rechercher attentivement quelque chose[283]. Ce « quelque chose » peut effectivement consister à vérifier que l'origine de la mort d'une personne ou de sa disparition inquiétante n'est pas le fruit d'une infraction. Le raisonnement est identique dans le cas d'une personne en fuite.

187. Dans ces trois cas, les investigations prévues par les articles 74 et suivants prévoient qu'il peut être procédé aux investigations prévues aux articles 56 à 62 du Code de procédure pénale, qui comportent plusieurs investigations numériques[284].

188. Conclusion de la section 2 : l'erreur d'une définition par la preuve numérique. – La facilité qui voudrait que « l'investigation numérique » soit définie comme l'investigation qui révèle des preuves numériques doit être écartée. Même si ces deux notions sont le plus souvent liées, les deux ensembles contenant ce à quoi elles se réfèrent, ne sont pas identiques. Certaines preuves numériques peuvent ne pas provenir

---

[279] V. *supra* n°1.

[280] C. pr. pén. art. 74 : « Dans ce cadre et à ces fins, il peut être procédé aux actes prévus par les articles 56 à 62, dans les conditions prévues par ces dispositions. »

[281] C. pr. pén. art. 74-2 : « Les officiers de police judiciaire, assistés le cas échéant des agents de police judiciaire, peuvent, sur instructions du procureur de la République, procéder aux actes prévus par les articles 56 à 62 aux fins de rechercher et de découvrir une personne en fuite […]. »

[282] C. pr. pén. art. 74-1 : « Lorsque la disparition d'un mineur ou d'un majeur protégé vient d'intervenir ou d'être constatée, les officiers de police judiciaire, assistés le cas échéant des agents de police judiciaire, peuvent, sur instructions du procureur de la République, procéder aux actes prévus par les articles 56 à 62, aux fins de découvrir la personne disparue […]. »

[283] V. *supra* n°111.

[284] C. pr. pén art. 56 à 57-1 pour la perquisition, notamment sur un environnement informatique : v *infra* n°244. pour une étude de ces actes.
C. pr. pén. art. 60-1 et 60-2 pour obtenir des données extraites d'un traitement de données à caractère personnel. V. *infra* n°372. pour une étude détaillée des mesures.

d'investigations numériques, de même que toutes les investigations numériques n'ont pas vocation à fournir des preuves.

189. Conclusion du chapitre 1 : l'absence de définition de l'investigation numérique. – Plus généralement, la notion d'investigation numérique est souvent perçue comme évidente par ceux qui l'emploient, alors que pour les techniciens, le grand public et dans les écrits juridiques, elle ne désigne pas forcément tout le temps la même chose. Par ailleurs, il existe un grand flottement au sein des textes et dans la doctrine autour des mots « numérique » et « électronique » qui génère un flou important sur les notions d'investigation et de preuve numériques.

190. Il n'existe donc pas, en l'état, de définition satisfaisante permettant de travailler de manière efficace et précise avec la notion d'investigation numérique en procédure pénale, de sorte qu'il est indispensable de préciser cette notion.

Chapitre 2. La définition de l'investigation numérique par des critères cumulatifs

191. Des critères définissant la notion et générant des conséquences spécifiques. – L'investigation numérique est une investigation qui a la particularité de manipuler des données informatiques[285]. Cette donnée doit être placée au cœur des critères définissant avec précision ce qu'est une investigation numérique. De plus, les données créent un environnement numérique. Cet environnement dématérialisé fait que les investigations numériques, dont l'objectif est de diligenter des techniques d'enquête sur des données, comportent des spécificités. Certaines sont des avantages dans le sens où elles rendent les investigations numériques plus faciles que des investigations classiques. Néanmoins, d'autres spécificités sont des contraintes propres à l'environnement numérique et doivent donc être prises en compte.

192. Il est donc nécessaire d'étudier les critères définissant la notion « d'investigation numérique » *(Section 1)* avant d'étudier les spécificités de l'environnement numérique dans lequel ces investigations sont réalisées *(Section 2)*.

Section 1. Des critères pour définir l'investigation numérique

193. Des critères pour définir et classer les investigations numériques en procédure pénale. – Afin de circonscrire parfaitement la notion « d'investigation numérique », il n'est possible de s'appuyer, ni sur les définitions des mots eux-mêmes, ni sur l'usage qui est fait de cette appellation aussi bien par le grand public que dans les écrits juridiques, qu'ils soient doctrinaux ou légaux et réglementaires[286].

La complétude de la notion est atteinte au travers de critères qui permettent de définir précisément et sans ambiguïté ce qu'est une investigation numérique en procédure pénale *(§1)*. Néanmoins, un critère supplémentaire doit être pris en compte afin de répartir ces investigations en deux catégories, utiles pour l'étude de leurs régimes *(§2)*.

[285] V. *supra* n°2.
[286] V. *supra* n°106. et s.

§1. Les critères intrinsèques de la notion

194. Les deux critères objectifs de définition. – En procédure pénale, la notion d'investigation numérique se définit par deux critères cumulatifs. En premier lieu, celle-ci ne peut exister que si une enquête judiciaire a préalablement été ouverte, quelle qu'en soit la raison et quelle qu'en soit la forme. Une investigation numérique en procédure pénale est donc, avant tout, un acte de procédure *(I)*.

En second lieu, cette mesure d'investigation, pour être numérique, doit recueillir ou générer des données au cours de son exécution *(II)*.

I – Un acte de procédure

195. Le pouvoir d'investigation comme prérogative exclusive des autorités judiciaires. – En France, à la différence des pays de droit anglo-saxon, seules les autorités judiciaires procèdent[287] à des investigations en procédure pénale[288]. Ce sont majoritairement les enquêteurs qui les mettent en œuvre, même si les magistrats peuvent procéder par eux-mêmes à certaines investigations[289].

196. En conséquence, le premier critère définissant une investigation numérique est qu'il s'agit d'un acte de procédure, à savoir un acte dûment prévu par une disposition légale[290], et dont la mise en œuvre et l'exécution sont également encadrées par des dispositions légales ou règlementaires[291]. Cet acte ne peut être ordonné et exécuté qu'au sein d'une procédure pénale officiellement ouverte, quelle qu'en soit la forme : enquête préliminaire, de flagrance, information judiciaire, enquête en cas de découverte d'un cadavre, aux fins de recherche des causes de la mort, recherche d'une personne en fuite ou disparue de manière inquiétante[292]. Dans ce contexte et comme cela a été précédemment expliqué[293], l'objectif des investigations numériques va au-delà de la recherche d'une preuve numérique puisque sa finalité est plus générale : contribuer à la résolution de la procédure en cours[294].

---

[287] Une variante consiste à ce que ces autorités judiciaires fassent procéder à des investigations par un tiers particulier, comme c'est le cas avec les experts : voir *infra* n°300.

[288] FIORINI Benjamin, *L'enquête pénale privée, Etude comparée des droits français et américain, Institut Universitaire Varenne*, Collection des Thèses, 2018, préface : « […] dans ce pays [les Etats Unis] l'enquête privée est « structurelle », alors qu'en France elle est encore un mode marginal de collecte des preuves. »

[289] Par exemple, un juge d'instruction peut demander à un tiers de lui communiquer directement des éléments (C. pr. pén. art. 99.3). Dans le cas des JIRS (juridictions interrégionales spécialisées), les magistrats sont parfois eux-mêmes équipés de logiciels de rapprochement judiciaire : voir *infra* n°293.

[290] La légalité de l'acte. V. *supra* n°132.

[291] *Ibid.* La licéité de l'acte.

[292] V. *supra* n°185. C. pr. pén. art. 74, 74-1 et 74-2.

[293] V. *supra* n°178.

[294] V. *supra* n°1.

197. Les éléments fournis par les autres parties que les autorités judiciaires. – Certes, les parties (mis en examen, partie civile) autre que l'autorité judiciaire peuvent diligenter une « action » pour étayer leurs affirmations, mais en aucun cas il ne s'agira d'une « investigation » qui, en procédure pénale, ne peut être réalisée que par des enquêteurs ou des magistrats. La procédure pénale repose sur un système mixte entre la procédure accusatoire et la procédure inquisitoire[295]. Néanmoins, l'influence du système inquisitoire pour, notamment, la recherche de preuves diligentée par les autorités judiciaires est prépondérante ce qui induit une différence majeure avec la procédure civile, y compris dans le vocabulaire utilisé. Ainsi, au sein de cette dernière, il est d'usage de parler d'une partie qui procède, par elle-même, à des investigations numériques dans le cadre d'une procédure judiciaire[296]. Ce n'est pas le cas en pénal, où le mot « investigation » est réservé aux actions des autorités judiciaires.

198. Les éléments remis par les parties comme origine à une investigation numérique. – Dans le cas qui vient d'être évoqué, une partie peut donc remettre spontanément aux autorités judiciaires des éléments sous forme numérique[297] provenant de ses propres recherches, ou manœuvres[298]. Comme précédemment expliqué, il ne serait pas juste de parler « d'investigation numérique » pour qualifier ces recherches ou ces manœuvres. En revanche, si un magistrat (ou un enquêteur), à qui ces éléments sont remis, ordonne une expertise (ou réquisitionne un expert) pour analyser ces éléments, alors l'expert procèdera à une investigation numérique[299] parce qu'il y a eu un acte de procédure.

---

[295] MERLE Roger et VITU André, *Traité de droit criminel – Problèmes généraux de la science criminelle, Droit pénal général,* Editions CUJAS, 7ème édition, p.167 et s. (Titre II : les problèmes de forme de la politique criminelle).

[296] V. *supra* n°163. L'article 145 du C. pr. civ. peut permettre à une partie, dans le cadre d'une ordonnance sur requête, de faire procéder à des investigations dans le système d'information d'un tiers par un huissier et un expert en informatique. Certes, ce n'est pas la partie elle-même qui procède aux investigations, mais c'est principalement elle qui a défini, en amont, le contenu et la nature des informations à rechercher lorsqu'elle dépose sa requête auprès du Président de la juridiction civile compétente (TGI, Tribunal de commerce, Conseil des prud'hommes).

[297] Par ex., un enregistrement audio que la partie a elle-même réalisé ou qu'elle s'est procurée. Il peut aussi s'agir d'un ordinateur qu'une victime présumée remet spontanément à un juge d'instruction ou à un enquêteur en expliquant que les données contenues peuvent aider à retrouver les auteurs des faits qu'elle dénonce.

[298] Crim. 9 déc. 2015 n°14-87.835 (JurisData n°2015-027585) : un employeur avait installé une caméra pour surveiller, à son insu, une salariée qu'il soupçonnait d'actes malintentionnés à l'égard de son environnement informatique. Bien que les vidéos issues de cette surveillance aient été retenues par les juridictions pénales saisies de l'affaire, elles ne sont pas le fruit d'une investigation numérique.

[299] Voir *infra* n°300.

Ainsi, des données[300] remises par une partie et issues de ses propres recherches, peuvent aboutir à des investigations numériques, mais moyennant la décision préalable d'une autorité judiciaire. On notera que cette étape intermédiaire revêt une importance cruciale, tout particulièrement lors de l'information judiciaire, puisque le juge d'instruction pré-confirme[301] ainsi la recevabilité des éléments versés lorsqu'il en ordonne l'exploitation technique.

199. Cette situation confirme qu'en procédure pénale, une investigation numérique est obligatoirement un acte ou une mesure diligentée ou ordonnée par une autorité judiciaire. Il s'agit bien là d'une particularité du droit répressif, puisqu'il a été évoqué que ce critère n'était pas applicable à, notamment, la procédure civile.

200. Le cas particulier des enquêtes administratives. – En enquête administrative ou en matière de renseignement, de nombreuses recherches numériques peuvent être réalisées[302] pour obtenir des renseignements, tout particulièrement depuis la vague d'attentats ayant frappés la France, et le maintien de l'état d'urgence jusqu'au 31 octobre 2017[303]. La loi du 21 juillet 2016[304] est venue modifier l'article 11 de la loi du 3 avril 1955 relative à l'état d'urgence[305], en introduisant une perquisition numérique directement inspirée de ce qui est prévu dans le Code de procédure pénale[306]. Celle-ci est placée sous le contrôle du juge administratif ce qui, au demeurant, ne va pas sans soulever des problèmes[307] quant à l'éventuelle recevabilité des éléments qui seraient recueillis à cette occasion, dans une procédure pénale ultérieure.

---

[300] Ou tout support ou matériel contenant des données.

[301] Il reste souverain pour déclarer irrecevable lesdits éléments si, précisément, à l'issue des investigations qu'il a ordonnées, il constate que le support remis avait été corrompu ou n'était pas fiable.
C. pr. pén. art. 81 5ème al. : « Le juge d'instruction doit vérifier les éléments d'information ainsi recueillis. »

[302] V. par ex. C. séc. int. : l'intégralité du Titre V (« Des techniques de recueil de renseignement soumises à autorisation ») du Livre VIII.

[303] Qui a pris fin avec l'entrée en vigueur des dispositions introduites par la loi n°2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme.

[304] Loi n°2016-987 du 21 juillet 2016 prorogeant l'application de la loi n°55-385 du 3 avril 1955 relative à l'état d'urgence et portant mesures de renforcement de la lutte antiterroriste.

[305] Loi n° 55-385 du 3 avril 1955 relative à l'état d'urgence.

[306] Pour une étude détaillée des différentes mesures, v. *infra* n°250.

[307] Le Monde Spécial, 2 novembre 2017, *Un an, 11 mois et 18 jours d'urgence*, p. 2.
Aujourd'hui en France, 5 novembre 2017, *Terrorisme Adapter « nos règles » au « risque durable »*, p. 5 : « Le pouvoir administratif, dévolu au ministère de l'Intérieur, en sort renforcé face à celui des magistrats. Il reste dans nos vies quotidiennes un soupçon d'état d'urgence. »

201. La mince frontière entre enquête administrative et pénale. – Lors de la loi de 2015 relative au renseignement[308], le Conseil Constitutionnel a rappelé que « le recueil de renseignement au moyen des techniques [de renseignement définies dans le] 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 être mis en œuvre pour constater des infractions à la loi pénale, en rassembler les preuves ou en rechercher les auteurs.[309] » Ce rappel, certes clair d'un point de vue sémantique, peut rapidement trouver ses limites dans le concret des dossiers. En effet, « la distinction entre la prévention des infractions et la constatation de celles-ci est parfois ténue[310] ». Pour preuve, il est tout à fait loisible d'envisager, tout particulièrement en matière de terrorisme, que les services de renseignement mettent à jour des infractions pénales grâce à leurs outils (notamment ceux permettant de procéder à des recherches numériques), et que les éléments factuels qui en sont issus soient transmis aux autorités judiciaires en tant qu'éléments de preuve dans une procédure qui sera judiciaire au final.

202. Sur ce point, deux arrêts de la Cour de cassation de décembre 2016[311], montrent que le juge pénal est compétent pour contrôler la légalité des actes accomplis préalablement dans le cadre de procédures administratives, dès lors qu'une procédure judiciaire est ouverte sur leur fondement[312].

203. Les éléments issus d'une enquête administrative identiques à ceux fournis par une partie. – Ainsi, la recevabilité, au sein d'une procédure pénale, des éléments issus d'une enquête administrative est identique à celle d'informations fournies par une partie. En aucun cas, les recherches numériques directement réalisées dans le cadre d'une procédure administrative peuvent être considérées comme un acte faisant partie intégrante

---

[308] Loi n°2015-912 du 24 juillet 2015 relative au renseignement.
[309] Décision n° 2015-713 DC du 23 juillet 2015.
[310] LEPAGE Agathe, *un an de droit pénal des nouvelles technologies (Octobre 2014 – Octobre 2015),* LexisNexis, Droit pénal n°12, décembre 2015, chronique n°10.
[311] Crim. 13 déc. 2016 n° 16-84.794 : JurisData n°2016-026324 – JC Pénal, RIAS Nicolas, *Synthèse Principes généraux de la loi pénale*, al. 26.
Crim. 13 déc. 2016 n°16-82.176 : JurisData n°2016-026322.
[312] RIBEYRE Cédric, *État d'urgence - État d'urgence et procédure pénale : le juge pénal compétent pour contrôler les perquisitions administratives,* LexisNexis, Droit pénal n°3, Mars 2017, étude n°6 : « La chambre criminelle de la Cour de cassation affirme, sur le fondement de l'article préliminaire du Code de procédure pénale et de l'article 111-5 du Code pénal, la compétence du juge pénal pour contrôler la légalité des ordres de perquisitions administratives menées dans le cadre de l'état d'urgence. Les juridictions d'instruction saisies de procédures judiciaires ouvertes à la suite de telles perquisitions peuvent donc, le cas échéant, annuler les actes du dossier bien qu'ils reposent sur une décision de nature administrative soumise comme telle au contrôle du juge administratif. »

de l'enquête pénale, ce qui est confirmé par un arrêt de la chambre criminelle du 3 mai 2017[313]. En effet, « il incombe au juge répressif […] de répondre aux griefs invoqués par le prévenu à l'encontre de cet acte administratif, sans faire peser la charge de la preuve sur le seul intéressé et en sollicitant, le cas échéant, le ministère public afin d'obtenir de l'autorité administrative les éléments factuels sur lesquels celle-ci s'était fondée pour prendre sa décision ». En conséquence, les renseignements issus d'une enquête administrative, puis ultérieurement versés à une procédure judiciaire, sont considérés par le juge pénal de la même manière que des informations fournies par une partie autre que le ministère public ou les enquêteurs. En procédure pénale, ces renseignements ne sont donc pas obtenus par des investigations numériques, mais par des techniques de recherches externes à la procédure[314].

204. Conclusion du sous-paragraphe I : un acte de procédure. – Ce dernier est la source de toute investigation numérique en procédure pénale. En effet, au sein de celle-ci, l'investigation numérique est un acte de procédure diligenté par les autorités judiciaires, et en aucun cas par un tiers, fût-ce l'Etat lui-même.

205. Mais un deuxième critère est nécessaire pour qualifier de « numérique » une investigation, prenant en compte les nombreuses ambiguïtés qui naissent avec ce mot, qui souffre parfois d'une utilisation hasardeuse[315].

II – La forme digitale du résultat

206. L'investigation numérique au sein des investigations. – Une investigation numérique est avant tout une investigation[316]. Pour être une investigation numérique, le deuxième critère que doit respecter l'acte de procédure l'ordonnant, est qu'il doit aboutir à l'obtention de données[317].

---

[313] Crim. 3 mai 2017 n°16-86.155 : JurisData n°2017-008272 ; D. 2017, p. 1175, note G. Beaussonie ; Dr. pén. 2017, comm. 109, note J.-H. Robert.

[314] Comme dans le cas d'une perquisition ordonnées par le Juge administratif. V. HERRAN Thomas et LACAZE Marion, *Affirmation de la compétence du juge pénal dans le contrôle des perquisitions administratives*, Dalloz AJ pénal 2017 p.30.
Op. cit. Crim. 13 déc. 2016 n°16-82.176 : JurisData n°2016-026322 et Crim. 13 déc. 2016 n° 16-84.794 : JurisData n°2016-026324.

[315] V. *supra* n°115.

[316] V. *supra* n°196.

[317] Sur la notion de données, v. *supra* n°6.

207. La distinction entre l'obtention des données et la fin de l'acte. – La fin de l'acte en lui-même est matérialisé par la remise d'un rapport ou d'un procès-verbal[318]. Pour qu'une investigation soit numérique, il faut que des données aient été obtenues au cours de l'exécution de l'acte, et que ces informations numériques restent potentiellement disponibles lorsque cette mesure est terminée. C'est notamment le cas chaque fois qu'un scellé contenant un support digital accompagne le rapport ou le procès-verbal.

208. L'intérêt de disposer de données numériques. – En effet, ces données présentent un intérêt potentiel important pour l'efficacité de l'enquête car elles peuvent être exploitées ultérieurement, dans un environnement informatique[319].

209. L'obligation de disposer de données à la fin de l'exécution de l'acte. – Ainsi, lorsqu'une une investigation se déroule dans un environnement numérique mais lorsque les enquêteurs se limitent à procéder à des constatations actées dans un procès-verbal[320], il ne s'agit pas d'une investigation numérique.

210. En effet, au-delà de cet exemple, dans toutes les situations où des données informatiques ne sont plus disponibles au terme de l'investigation, on est en présence d'une investigation techniquement assistée, comme lorsque les enquêteurs utilisent des véhicules pour se rendre sur les lieux d'une perquisition ou pour aller auditionner un témoin, mais pas dans le cas d'une investigation numérique. Le fait que les outils utilisés soient technologiquement complexes ne permet pas, à lui seul, de qualifier de « numérique » une telle investigation.

211. Conclusion du paragraphe §1 : les critères intrinsèques de la notion. – La notion d'investigation numérique en procédure pénale repose, en premier lieu, sur le fait qu'elle désigne un acte d'enquête. Néanmoins, en second lieu, il s'agit d'un acte particulier, dont le régime abouti à l'obtention de données. Ces dernières peuvent avoir été recueillies comme, par exemple, lors d'une perquisition[321], ou générées comme dans

[318] PRADEL Jean, *Procédure pénale*, 19ème édition, Cujas, p.729 : « Ces actes doivent donner lieu à un procès-verbal, seul moyen d'en assurer la conservation. »

[319] Sur l'amélioration de l'exploitation des données saisies ou générées lors des différentes investigations numériques en enquête pénale, v. *infra* n°799.

[320] V. *supra* n°150. Par exemple, le cas d'enquêteurs qui utilisent un dispositif de « fixation d'images » mais se contentant de visualiser les images en temps réel sans enregistrer, ne constitue pas une investigation numérique, même s'ils dressent un procès-verbal décrivant ce qu'ils ont vus. Pour être une investigation numérique, il faut qu'un fichier vidéo soit versé à la procédure.

[321] Sur la perquisition et l'obtention de données, v. *infra* n°244.

le cas d'une géolocalisation[322]. L'intérêt de ces données, dont la durée de vie dépasse l'acte au travers duquel elles ont été obtenues, est que ces informations numériques offrent un potentiel d'investigation inexploité jusqu'à présent[323].

212. Les deux critères permettant de définir avec rigueur la notion d'investigation numérique en procédure pénale peuvent être complétés par un troisième, dont l'intérêt est de pouvoir classer ces investigations.

§2. Un critère secondaire discriminant

213. Les deux catégories d'investigations numériques. – Outre les deux critères cumulatifs permettant de définir, sans ambiguïté, ce qu'est une investigation numérique en procédure pénale, un critère supplémentaire permet de les classer en deux catégories. Celui-ci ne suffit pas, pris isolément, à cerner la notion car il est applicable à d'autres actes d'investigations. En revanche, il présente l'intérêt de différentier deux groupes d'investigations numériques, selon que l'acte à l'origine de la recherche des informations digitales est « intrusif par action » ou pas.

214. Les investigations avec les traitements de données judiciaires. – Comme cela a été expliqué précédemment[324], la multiplication des traitements de données mis en œuvre par l'Etat, dont les informations sont accessibles au cours de l'enquête pénale[325], fait des recherches au sein de ces fichiers une catégorie d'investigations numériques à part entière. Celles-ci sont des mesures non intrusives, puisque les enquêteurs extraient des données qui sont la propriété de l'administration. En effet, ces données sont enregistrées dans des traitements de données judiciaires ou administratifs[326]. Par voie de conséquence, les informations numériques obtenues avec la consultation de ces fichiers ne sont pas directement intrusives dans la vie privée de la personne ciblée par ces recherches. Avec la consultation des fichiers administratifs et judiciaires, l'enquêteur se place dans une démarche passive, sans action forte de sa part.

---

[322] Sur la géolocalisation, v. *infra* n°486.
[323] Pour l'efficacité des analyses de données ou de supports numériques saisis : v. *infra* n°740.
[324] V. *supra* n°153.
[325] Sur le critère de l'accès direct aux traitements judiciaires, v. *infra* n°612.
Crim. 15 septembre 2009 n°09-82.597 Bull. crim. 2009, n°155. Recueil Dalloz 2009 p.2428, *La consultation des fichiers de police ne nécessite pas de réquisition.*
[326] V. *infra* n°636.

215. Une action intrusive forte de la part des enquêteurs. – La deuxième famille regroupe toutes les investigations numériques qui se situent à la réunion des mesures coercitives et intrusives, et pour lesquelles les autorités judiciaires accomplissent des actions fortes et actives dans leur recherche d'éléments.

216. Conclusion de la section 1 : des critères pour définir l'investigation numérique. – Une investigation numérique en procédure pénale est un acte de procédure dument prévu par les textes et ordonné par une autorité judiciaire, qui permet l'obtention ou la génération de données potentiellement disponibles pour la suite de l'enquête.
Un critère supplémentaire, reposant sur le fait que les données recueillies sont issues de la consultation des traitements de données mis en œuvre par l'Etat ou le fruit d'actes d'investigations coercitifs ou intrusifs, permet de distinguer deux familles d'investigations numériques. Cette distinction présente un intérêt majeur pour l'étude de leurs régimes[327].

Section 2. Des spécificités pour préciser l'investigation numérique

217. Les spécificités de l'environnement des investigations numériques. – Au-delà des critères définissant rigoureusement ce qu'est une investigation numérique en procédure pénale, celle-ci possède des spécificités qui, certes, ne permettent pas de la définir[328], mais qui créent un environnement unique, au sein duquel les investigations numériques sont diligentées. Ce contexte particulier découle directement de la notion d'investigation numérique. La donnée, centrale au sein de la notion, génère des contraintes et des avantages spécifiques[329].
Ces spécificités ont de fortes conséquences sur les investigations numériques, en générant principalement des contraintes aux autorités judiciaires *(§1),* même si le don d'ubiquité apporte, pour sa part, de la souplesse *(§2)*.

[327] V. *infra* n°233.
[328] D'autres investigations peuvent ponctuellement avoir ces mêmes spécificités. Par exemple, une trace ADN déposée dans un lieu ouvert au public doit être recueillie très rapidement au risque qu'elle soit polluée.
[329] Ce sont parfois les conditions de mise en œuvre de l'acte portant l'investigation numérique qui sont impactées, comme avec la volatilité qui impose une décision très rapide des autorités judiciaires. Mais cela peut-être également les effets de l'acte : les données d'un même disque dur peuvent être exploitées à deux endroits géographiquement distants au même moment.

§1. Les investigations gênées par certaines spécificités

218. Des contraintes spécifiques aux investigations numériques. – L'immatérialité *(I)* et la volatilité *(II)* sont deux caractéristiques intrinsèques des investigations numériques dont les conséquences sont majeures. La conséquence est principalement négative pour les autorités judiciaires, en imposant des contraintes temporelles et en soulevant des doutes sur la localisation géographique des données.

I – L'immatérialité des données informatiques

219. La confusion de l'assimilation de la donnée et du microscopique. – Les investigations dans un environnement informatique ne doivent pas être confondues avec celles qui ont pour objet « l'infiniment petit ». Elles sont souvent comparées, à tort, avec des analyses génétiques[330] ou chimiques (de cheveux[331], de sang, etc), sans doute en raison de l'aspect « non visible à l'œil nu » qu'elles ont en commun. Pour autant la comparaison s'arrête là. En effet, bien que microscopiques, les résultats d'analyses ADN s'appuient sur des éléments matériels du corps humain. Il en va de même pour les analyses chimiques qui révèlent la présence « physique » de telle ou telle substance dans l'organisme[332]. L'investigation numérique diffère en ceci qu'elle recherche des informations qui n'ont pas d'existence physique, puisque les niveaux électriques ou magnétiques qui permettent le stockage d'un bit[333] sur un support digital, sont inintelligibles sans une couche électronique, nommée « contrôleur », qui donne un sens informatif à ces bits[334].

220. D'autres auteurs préfèrent le terme « d'incorporel » à celui « d'immatériel »[335]. En droit civil un bien incorporel est défini comme un bien immatériel, ce qui lève toute ambiguïté sur la synonymie de ces deux mots. En résumé, l'immatérialité qui entoure une investigation numérique signifie que l'élément digital qui est sa cible n'est pas tangible.

221. L'incertitude de la localisation des données. – De plus, cette immatérialité se trouve désormais exponentiellement accentuée avec les hébergements de type *cloud*

---

[330] Dossier : La preuve génétique, Dalloz AJ pénal 2018 p.59.
[331] REVENIER Jean-Loup, *Quand les cheveux « parlent »,* Le Point n°1314, 22 nov. 1997 : « […] l'analyse des cheveux par la chromatographie en phase gazeuse couplée à la spectrométrie de masse, apportent aux investigateurs judiciaires des réponses décisives. »
[332] BESACIER Fabrice, *Trafic de stupéfiants : une approche scientifique*, Dalloz AJ pénal 2006 p.251.
[333] V. *supra* n°116. Un bit ne peut prendre que deux valeurs (0 ou 1).
[334] V. *supra* n°9.
[335] MICHALSKI Cédric, *La recherche et la saisie des preuves électroniques*, Gazette du Palais 11 fév. 2014 n°42 p.12.

computing, qui consistent à héberger des données ou des applications[336], en permettant d'y accéder depuis n'importe quel ordinateur connecté à Internet[337]. Bien entendu, cet accès potentiel peut être encadré par des procédures techniques et organisationnelles plus ou moins sécurisées[338]. Néanmoins, ce type d'hébergement suppose que la continuité de service soit assurée, ce qui a pour conséquence que les grands hébergeurs de données possèdent plusieurs *Data Center* se répliquant les uns les autres, afin qu'en cas de défaillance d'un site, un autre site géographiquement distant puisse prendre le relais. Ce sont donc ces techniques de réplication et de déduplication[339] des données qui accentuent profondément l'immatérialité de l'information, puisque l'utilisateur qui y accède ne sait pas où cette dernière est physiquement stockée au moment où il la visualise sur son terminal.

222. Les conséquences de l'immatérialité sur les investigations. – Cette immatérialité qui entoure les investigations numériques a des répercussions immédiates. Par exemple, elle oblige constamment à s'interroger sur la localisation des données, tout particulièrement dans le cas de leur extraterritorialité, puisque l'article 57-1 du Code de procédure pénale prévoit que « […] les officiers de police judiciaire […] peuvent, au cours d'une perquisition […], accéder par un système informatique implanté sur les lieux où se déroule la perquisition à des données intéressant l'enquête en cours et stockées dans ledit système, dès lors que ces données sont accessibles à partir du système initial ou disponibles pour le système initial[340] ».

---

[336] On parle alors de fonctionnement en mode SAAS comme « Software As A Service ». L'utilisateur de la ressource se connecte à son application à distance, sans installer physiquement un logiciel sur son propre ordinateur.

[337] FRANSSEN Vanessa, *The European Commission's E-evidence Proposal : Toward an EU-wide Obligation for Service Providers to Cooperate with Law Enforcement ?*, European Law Blog, 12 octobre 2018 : "[…] the increased use of all kinds of online services and information and communication technologies (ICTs), police et judicial authorities are confronted on a daily basis with the problem to collect electronic evidence, as the data they are looking for are often processed, transmitted and stored by foreign providers […]".
Sur les effets juridiques du *cloud*, v. eg. BRUNAUX Geoffray, *Cloud computing, protection des données : et si la solution résidait dans le droit des contrats spéciaux ?*, Recueil Dalloz, 2013 p.1158.

[338] V. *infra* n°265.

[339] Pour vulgariser, la déduplication est une sorte de compression des données destinée à améliorer le stockage. Par un principe de découpage des fichiers et de factorisation des séquences binaires, elle rend les données stockées totalement inintelligibles.

[340] Sur la localisation des données, v. *infra* n°260.

II – La volatilité des données informatiques

223. La facilité d'effacement et de modification des données. – L'aspect volatil, terme auquel d'autres auteurs préfèrent le mot « fugace »[341], est sans nul doute le plus intuitif et le premier qui vient à l'esprit, puisque, spontanément, on pense à Internet où les informations peuvent apparaître et disparaître (ou être modifiées[342]) en quelques instants. Bien que des propos diffamatoires[343] au sens de l'article 29 de la loi du 29 juillet 1881 sur la liberté de la presse puissent se diffuser en quelques heures s'ils font le *buzz*, la cible de ces propos peut éprouver des difficultés pour se pré-constituer une preuve. En effet, dans ce type de situation, le réflexe juridique consiste à faire appel à un Huissier de justice pour procéder à un constat sur Internet[344]. Or, les propos initiaux peuvent être retirés au bout de quelques heures, à savoir avant que le constat ait été réalisé : la victime aura du mal à prouver ses dires, surtout pour ce qui est de l'imputabilité à leur auteur originel, alors que les effets négatifs des allégations perdureront.

224. On peut également inclure dans la notion de volatilité la facilité avec laquelle peuvent être supprimées, et donc dissimulées, des quantités très importantes de données. Certes, il existe des logiciels spécifiques pour rechercher les fichiers supprimés sur des supports numériques, mais dont le champ d'application se limite aux disques durs d'ordinateurs précédemment mis sous scellés[345]. De plus, d'une part, ces recherches sont de plus en plus contrariées par les logiciels de cryptage[346] et d'effacement sécurisé que l'on trouve gratuitement sur Internet et faciles à installer et, d'autre part, l'utilisation des logiciels d'investigation est inapplicable si les données supprimées l'ont été sur les serveurs d'un hébergeur externe, notamment dans *le cloud*[347].

225. Le besoin de réactivité des investigations. – La volatilité de l'environnement numérique sous-entend une grande facilité de suppression d'éléments. Il en résulte un besoin de vitesse dans la recherche et la collecte des éléments, ce qui, au sein investigations numériques intrusives par action, a de fortes conséquences sur tous les

---

[341] *Op. cit.* p. 35 - QUEMENER Myriam, *Les spécificités juridiques de la preuve numérique*.
[342] La modification est une variante de la suppression (puisque la modification revient à supprimer l'état antérieur de l'information) parfois pire que la suppression elle-même. En effet, il est souvent plus difficile de retrouver l'historique d'une donnée à un instant « t », qu'une donnée qui a été effacée. Dans ce cas, en effet, soit on retrouve la donnée soit on ne la retrouve pas. Dans le cas de la modification, la question récurrente est de savoir si l'on a bien retrouvé tous les états antérieurs de l'information recherchée.
[343] Par exemple, sur un blog ou un forum.
[344] V. *infra* n°476.
[345] Pour les investigations réalisées sur les supports numériques, v. *infra* n°293.
[346] V. *infra* n°431.
[347] V. *supra* n°221. et *infra* n°258.

actes contribuant à la recherche de données créées ou générées par des suspects, et sur lesquels ceux-ci ont le contrôle, au sens informatique de terme[348].

226. Ainsi, la volatilité est la principale justification des actes permettant la mise en œuvre d'investigations numériques particulièrement attentatoires aux libertés individuelles[349].

§2. Les investigations facilitées par la spécificité de l'ubiquité

227. La facilité de cloner les informations numériques. – La donnée ne présente pas que des inconvénients pour les investigations numériques. On dit d'un bien qu'il est non rival[350], s'il possède le don d'ubiquité[351]. C'est le cas des données puisqu'elles peuvent être clonées avec une fidélité exacte, à tel point qu'il est impossible, dans la majorité cas, de distinguer la copie du support original. Ceci a deux conséquences, très positives, lorsqu'on s'intéresse aux investigations numériques.

228. La protection de la donnée. – En premier lieu, cela signifie que l'on peut préserver facilement un support informatique, puisque l'on peut le « cloner[352] » et donc diligenter des investigations sur l'image ainsi réalisée, sans risquer de détériorer le support initialement saisi.

229. La simultanéité d'investigations géographiquement distante sur une même donnée. – En second lieu, en cas de besoin, des copies fidèles d'un support numérique peuvent être réalisées, permettant ainsi à deux personnes (ou plus) géographiquement distantes, de procéder à des investigations sur les mêmes données au même moment, sans avoir à détériorer ou à faire voyager le support d'origine. Par exemple, le juge d'instruction peut rendre une ordonnance de dualité d'expert en informatique[353] : les deux

[348] V. *supra* n°171. Christiane FERAL SCHUHL évoque les délinquants qui peuvent facilement détruire et déplacer des données. FERAL SCHUHL Christiane, *La collecte de la preuve en matière pénale* (*op. cit.* p.35).
[349] Pour les investigations numériques intrusives, v. *infra* n°235.
[350] Notion définie par les économistes. V. ALAMAR Bruno, *Pour la libre circulation des données*, Le monde Eco et Entreprise, 11 avril 2018 : « […] la donnée est un bien « non -rival », c'est-à-dire un bien qui, une fois consommé par les uns, existe encore pour les autres. »
[351] Dicitonnaire Larousse : « Fait d'être présent partout à la fois ou en plusieurs lieux en même temps. »
[352] Mot employé par les informaticiens en référence au clonage (dictionnaire Larousse : « Technique permettant d'obtenir en laboratoire des lignées de cellules ou des embryons à partir d'une cellule, sans qu'il y ait fécondation. ») pour qualifier la copie d'un support avec une reproduction exacte de son contenu.
[353] Pour la commission et la réquisition des experts, v. *infra* n°301.

experts peuvent se répartir des tâches précises sur des données identiques, préalablement clonées depuis un même support d'origine.

230. Conclusion du titre 1 : la nécessité de définir la notion « d'investigation numérique ». – La dématérialisation de notre société pénètre l'ensemble des domaines professionnels. Dans l'exercice de la justice, cette dématérialisation se traduit, notamment[354], par la dématérialisation de la recherche des preuves lors des procédures pénales. Les recherches des preuves dématérialisées constituent ce que l'on nomme les investigations numériques. Or, l'utilisation de l'appellation « investigation numérique », aussi bien par les techniciens que dans la doctrine juridique, révèle qu'elle est perçue comme une évidence, alors qu'un flou important entoure ce que les auteurs désignent concrètement lorsqu'ils l'emploient[355]. Ce flou provient principalement du mot « numérique » qui est souvent confondu avec « électronique ».

231. Pour définir parfaitement la notion « d'investigation numérique » en procédure pénale, il est nécessaire d'énoncer deux critères cumulatifs. En premier lieu, elle est un acte de procédure ordonné par les autorités judiciaires. En second lieu, pour être numérique, une investigation doit avoir pour effet d'obtenir ou de générer des données potentiellement disponibles pour la suite de l'enquête.

232. Un troisième critère vient les classer en deux groupes. Tout d'abord, une première catégorie permet de verser au dossier des données qui sont recueillies à la suite d'une demande ou d'une consultation de traitements de données à caractère personnel. Ensuite, une seconde catégorie regroupe l'ensemble des actes d'investigations coercitifs ou intrusifs, qui se caractérisent par une action forte de la part des enquêteurs. Ce classement est utile pour l'étude du régime des différentes investigations numériques. En effet, les spécificités que sont l'immatérialité et la volatilité des données s'imposent aux investigations numériques. Ces deux spécificités ont une répercussion importante sur la seconde catégorie, puisqu'elles justifient le caractère fortement attentatoire aux libertés individuelles.

[354] Une autre conséquence est la dématérialisation « administrative » de la procédure : v. *supra* n°43.
[355] V. *supra* n°128. et 148.

TITRE II. LE CONSTAT DE LA PLURALITE DES REGIMES

233. Les deux catégories d'investigations numériques. – Les investigations numériques en procédure pénale sont des actes qui ont pour effet d'obtenir ou de générer des données potentiellement disponibles pour la suite de l'enquête. Les données qui sont obtenues à partir de la consultation des traitements de données à caractère personnel judiciaires définissent une catégorie d'investigations numériques. Une autre catégorie regroupe les investigations qui ont permis la génération ou la saisie de données au travers d'actes d'enquêtes coercitifs ou fortement intrusifs.

234. Une multitude de régimes. – Le point en commun de ces deux groupes d'investigations numériques est que les actes permettant de les mettre en œuvre ont été créés sans réflexion de fond et sans cohérence[356]. La conséquence est qu'une multitude de régimes apparaît lorsque ces actes sont étudiés.

Pour autant, il convient de distinguer les régimes des investigations numériques intrusives et souvent coercitives *(Chapitre 1)*, de ceux des investigations numériques d'extraction d'informations digitales depuis des traitements de données judiciaires *(Chapitre 2)*.

[356] V. *supra* n°83.

Chapitre 1. Les régimes de l'obtention de données par des actes intrusifs

235. Des investigations reposant sur une action forte des enquêteurs. – Les investigations numériques intrusives sont des actes permettant la recherche d'informations par des actions fortes, parfois coercitives. C'est au sein de celles-ci que sont présents la majorité des actes permettant de procéder à des investigations numériques. Par « majorité », on se réfère uniquement à leur quantité, sans y mettre une quelconque connotation d'importance ou de fréquence d'utilisation par les autorités judiciaires.

236. C'est un véritable arsenal procédural qui est aujourd'hui mis à la disposition des enquêteurs pour procéder à des investigations numériques intrusives.

237. Des investigations éparpillées dans le Code de procédure pénale. – Ces nombreux actes sont présents, aussi bien au sein des procédures dérogatoires, notamment celles qui sont prévues en matière de criminalité organisée ou de terrorisme, que dans les actes de l'information judiciaire, ou encore dans d'autres catégories de dispositions spécifiques[357]. Même si la loi du 23 mars 2019[358] a amorcé une meilleure organisation[359], notamment des investigations numériques, l'éparpillement de ces actes au sein du Code de procédure pénale reste très important.

238. Des régimes différents. – Cet éparpillement des investigations numériques dans le Code est inextricablement associé à une multitude de régimes pour les actes correspondants. La loi du 23 mars 2019 avait pour ambition d'homogénéiser ces régimes, mais les censures partielles du Conseil constitutionnel[360] ont « détricoté la loi[361] »,

[357] V. par ex. la géolocalisation ou l'enquête sous pseudonyme qui sont prévues dans un titre IV intitulé « dispositions communes ».
[358] Loi n°2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice
[359] Ce sont, notamment, les actes prévus pour « la procédure applicable à la criminalité et à la délinquance organisées et aux crimes », pour lesquels la loi du 23 mars 2019 a introduit des dispositions communes évitant les nombreuses répétitions entre les différentes investigations numériques quant aux rôles du juge des libertés et de la détention et du juge d'instruction.
Op. cit. p.19. VERGES Etienne, *Réforme de la procédure pénale : une loi fleuve, pour une justice au gré des courants.*
[360] Conseil constitutionnel, décision n°2019-778 DC du 21 mars 2019.
[361] *Ibid* . VERGES : « Il s'agissait […] d'harmoniser en parties les différents régimes applicables. […] Du point de vue de la simplification et de la cohérence, le projet était louable, mais l'ambition d'efficacité a été portée au-delà de ce que le Conseil constitutionnel pouvait tolérer. »

laissant subsister des régimes différents aussi bien dans leurs conditions de mise en œuvre que dans les subtilités qui perdurent au sein des procédures dérogatoires au droit commun.

239. Dès lors, il n'existe pas d'autres moyens que de procéder à une étude exhaustive de tous les actes permettant de déclencher les investigations numériques intrusives afin d'en recenser l'ensemble des régimes applicables.

240. Une difficulté de classement. – Parmi l'ensemble de ces actes, il est difficile de réaliser une classification logique et rationnelle[362]. Certains auteurs optent pour un classement selon un « répertoire ordinaire[363]», qui regroupe les actes prévus pour la procédure de droit commun et un « répertoire ajouté[364] » pour les procédures réservées à des infractions précisément définies. Pour recenser les investigations numériques intrusives et étudier leurs régimes, cette répartition n'est pas pertinente car leur éparpillement dans le Code de procédure pénale rend ce classement inefficace : des dispositions sont présentées en enquête, d'autres à l'information judiciaire, d'autres encore dans les dispositions communes aux procédures de droit commun et, enfin, dans les procédures réservées à la criminalité organisée.

241. Un classement selon la façon d'obtenir les données. – Dans le cadre de la présente étude, il est préférable de répartir les investigations numériques selon la méthode qui permet d'obtenir des données. Une première catégorie regroupe les données qui sont traitées lors d'actes de fouilles. Le mot « fouille » se réfère à l'action « d'explorer minutieusement un lieu pour trouver quelque chose, quelqu'un[365]». En procédure pénale, ce mot est fréquemment utilisé[366], dans un sens conforme à la définition littéraire. Dans le cas des investigations numériques, il s'agit de fouiller des supports contenant des

---

[362] GUINCHARD Serge et BUISSON Jacques, *Manuel de Procédure pénale*, (*op. cit.* p.31) p. 525 : « Rejetant tout classement entre modes de preuve, aléatoire en théorie et inutile en pratique, nous considérons comme plus opératoire de reprendre chacun des actes d'administration de la preuve ou modes de preuve exécutés par les agents de l'autorité publique, sans autre préoccupation que de livrer une description du « répertoire » dans lequel ces agents doivent choisir pour la recherche et le recueil des indices. »

[363] *Ibid.* Le répertoire ordinaire regroupe « les actes d'administration de la preuve que la loi a déterminée pour le recueil des indices nécessaires à toutes les infractions, quelles qu'elles soient, prévues par le Code pénal ou par des lois spéciales. »

[364] BUISSON Jacques, *Preuve* (*op. cit.* p.35), al. 229 : « par cette expression de répertoire ajouté, nous entendons la liste des actes d'administration de la preuve […] pour le recueil des indices nécessaires à l'établissement des infractions […] limitativement énumérées. »

[365] Source : dictionnaire Larousse

[366] C. pr. pén. art. 63-6 et 63-7 régime de la fouille lors d'une garde à vue.
C. pr. pén. art. 78-2-2 III : fouille des bagages.

données. Une seconde catégorie réunit les données qui sont générées ou collectées lors de l'exécution d'actes de surveillance. Cette surveillance est tout aussi intrusive dans la vie privée que les actes de fouille, mais elle se déroule systématiquement à l'insu de l'individu visée par la mesure.

242. Le recensement et l'étude des régimes des actes aboutissant à l'obtention de données par des fouilles *(section 1)* sont donc distingués de ceux de la génération et la collecte de données au travers des mesures de surveillance *(section 2)*.

Section 1. L'obtention de données par des actes de fouille

243. De nombreux actes pour fouiller des données. – En premier lieu, c'est la perquisition qui représente le mieux cette notion de fouille. Il s'agit d'un acte complexe offrant de larges possibilités aux enquêteurs. Il comporte explicitement la possibilité d'investiguer dans des données. En second lieu, la notion de fouille d'informations numériques est présente dans plusieurs autres mesures. Parfois, la fouille n'est pas explicitement mentionnée, mais la formulation des dispositions l'autorise clairement dans les données visées par l'acte.

En conséquence, l'étude de la perquisition, acte central de la procédure pénale *(§1)*, est distinguée des autres actes autorisant des fouilles de données *(§2)*.

§1. La perquisition

244. Un acte aux très larges effets. – La perquisition est prévue dans le Code de procédure pénale aux articles 56, 76 et 92 et suivants[367]. Les pouvoirs sont étendus lors de l'information judiciaire, notamment pour les lieux susceptibles d'être ciblés par la perquisition[368]. La définition de la perquisition est jurisprudentielle : « toute perquisition implique la recherche, à l'intérieur d'un lieu normalement clos, notamment au domicile d'un particulier, d'indices permettant d'établir l'existence d'une infraction et d'en déterminer l'auteur[369] ».

245. Elle est l'une des mesures les plus importantes dans les enquêtes aussi bien policières que judiciaires. Elle a pour vocation de permettre la saisie d'indices ou de tout

[367] Respectivement, en enquête de flagrance, en enquête préliminaire et pour les juridictions d'instruction.
[368] C. pr. pén., art. 94 : « Les perquisitions sont effectuées dans tous les lieux où peuvent se trouver des objets ou des données informatiques dont la découverte serait utile à la manifestation de la vérité […]. »
[369] Crim. 29 mars 1994 n°93-84.995. JurisData n°1994-000789 ; Dr. pén. 1994, chron. 40 et comm. 194. – 20 sept. 1995 : Bull. crim. 1995, n° 276 ; D. 1996, somm. p. 256, note Pradel.
PRADEL Jean, *Définition de la perquisition : notion de lieu clos,* Recueil Dalloz 1995 p.144.

élément susceptible d'être en rapport avec les faits qui sont à l'origine de la procédure. Elle peut avoir aussi pour finalité la saisie conservatoire ou des confiscations en application de l'article 131-21 du Code pénal, mais ceci est extérieur à la présente étude.

246. Les deux degrés de dématérialisation de la perquisition. – La perquisition repose sur deux séries de mesures, directement liées au potentiel d'investigation sur les données. En premier lieu, la perquisition « classique » *(I)* prévue par les articles 56, 76 et 92 permet de saisir directement des données ou des objets qui en contiennent. En second lieu, la « perquisition en ligne » *(II)* définie aux articles 57-1, 77-1-1 et 97-1, doit être distinguée car elle prévoit la fouille et la saisie de données au travers d'un réseau informatique.

I – La perquisition « classique »

247. La prise en compte des données dans la perquisition. – Le champ de la perquisition est, bien évidemment, beaucoup plus vaste que les investigations numériques[370]. Toutefois, le Code de procédure pénale leur consacre plusieurs spécificités qui offrent aux enquêteurs procédant à la perquisition, des moyens dédiés à la recherche d'informations numériques susceptibles d'intéresser les faits.

248. La saisie classique d'un objet. – Des objets retrouvés au sein du local, objet de la perquisition et susceptibles d'intéresser les faits, peuvent être saisis. Dans ce cadre, des supports digitaux contenant des données[371] sont des objets comme les autres et ils peuvent donc être appréhendés. Il ne s'agit pas d'une investigation numérique à proprement parler puisque, à ce stade, aucune analyse[372] n'est réalisée. Les officiers de police judiciaire se contentent de mettre sous scellés des ordinateurs ou autres supports numériques (appareils photos, cartes mémoires, disques durs externes, téléphones, etc) pouvant contenir des

[370] C. pr. pén. art. 56 en enquête de flagrance : « Si la nature du crime est telle que la preuve en puisse être acquise par la saisie des papiers, documents, données informatiques ou autres objets […]. » Outre la saisie des éléments incorporels que sont les données (v. *supra* n°219.), la perquisition a pour objet de saisir des éléments physiques, tangibles.

[371] Crim. 21 Mars 2018 n°16-87.193, inédit : « […] la saisie de documents ou tout support d'information comprend la faculté de saisir le support lui-même, ordinateur ou disque dur, ou de prendre copie de l'information sur un support externe ; qu'aucun reproche ne peut donc être fait en l'espèce aux enquêteurs d'avoir démonté les ordinateurs. »

[372] V. *infra* n°294. .

informations intéressantes pour l'enquête[373]. La démarche est identique à celle de la saisie d'une arme ou d'un objet suspecté d'avoir servi à commettre une infraction, et dont les traces de sang ou d'ADN ne peuvent pas être exploitées pendant la perquisition. Les véritables investigations sur ces supports seront donc réalisées ultérieurement[374].

249. La saisie directe de données au cours de la perquisition. – Les alinéas 5 à 7 de l'article 56 (au stade de l'enquête[375]) et l'article 97 (lors de l'instruction) prévoient la saisie directe de données trouvées lors de la perquisition. Pour autant, la portée de ces dispositions reste limitée car il est difficile de procéder à des investigations numériques en temps réel lors d'une perquisition. Les données informatiques étant très volatiles[376], le risque de les détériorer est important. C'est pourquoi, usuellement, les officiers de police judiciaire procèdent plutôt à la saisie des supports et en diffèrent l'analyse[377] dans un environnement technique adapté, afin d'en préserver l'intégrité[378].

II – La perquisition « en ligne »

250. La dématérialisation de la perquisition. – En termes d'investigations numériques diligentées au cours d'une perquisition, ce sont les dispositions de l'article 57-1, prévues dans le cadre des enquêtes de flagrance[379] qui offrent le plus de possibilités. En effet, cet article crée une véritable « perquisition en ligne[380] » au sein de la perquisition, puisqu'il est permis « d'accéder à un […] système informatique [distant] dès lors que ces données sont accessibles à partir du système initial ou disponibles pour le système initial ». Même lorsqu'une information judiciaire est ouverte, et au sein de laquelle les puissants pouvoirs d'investigation offerts au juge d'instruction lui permettent de perquisitionner « dans tous les lieux où peuvent se trouver […] des données

[373] C. pr. pén. art. 56 en enquête de flagrance : « Tous objets et documents saisis sont immédiatement inventoriés et placés sous scellés ». - Art. 76 en enquête préliminaire : « Les dispositions prévues par les articles 56 […] sont applicables ». Art. 97 lors de l'instruction : « Tous les objets […] placés sous main de justice sont immédiatement inventoriés et placés sous scellés. »
[374] *Ibid.*
[375] L'article 56 du C. pr. pén concerne les enquêtes de flagrance mais les dispositions citées sont étendues à l'enquête préliminaire au travers de l'article 76 *(3ième alinéa)*
[376] Sur la volatilité des données informatiques : v. *supra* n°223.
[377] V. *infra* n°294.
[378] A savoir dans un environnement permettant un clonage du support saisi au travers d'un bloqueur en écriture, et composé de logiciels d'investigation permettant des analyses de données, le plus souvent longues à réaliser et donc incompatibles avec la durée d'une perquisition.
[379] Etendues aux enquêtes préliminaires et à l'instruction au travers des articles 76-3 et 97-1 du C. pr. pén.
[380] Sophie SONTAG parle de « perquisition 2.0 ». V. SONTAG KOENIG Sophie, *Les perquisitions 2.0 : quand l'informatique se saisit de l'immatériel.* (*op. cit.* p.35).

informatiques dont la découverte serait utile à la manifestation de la vérité[381] », l'article 97-1 (qui renvoie à l'article 57-1), reste très intéressant.

251. Un accès à distance à des données précisément défini. – La Cour de cassation a eu l'occasion de préciser la notion d'accès à un système informatique distant. En effet, la découverte d'éléments non numériques lors d'une perquisition ont permis aux enquêteurs de se connecter ultérieurement à un site Internet. Un pourvoi fut formé au motif que cet accès à un site Internet par les officiers de police judiciaire aurait dû être réalisé dans le cadre d'une perquisition informatique en application de l'article 57-1. La Cour de cassation, dans un arrêt du 6 novembre 2013 publié au bulletin[382], a répondu par la négative, précisant que le fait, pour des enquêteurs, de se connecter à un site Internet avec les identifiants d'un suspect retrouvés sur des notes manuscrites lors de la perquisition, n'entrait pas dans le champ d'application de l'article 57-1, et ne constituait qu'une « simple investigation[383] ».

252. Une limitation par la réalité du terrain. – Pour leur part, les dispositions de l'article 57-1 ont peu d'utilités pour les perquisitions réalisées aux domiciles des particuliers. Elles trouvent tout leur sens et toute leur pertinence pour les perquisitions en environnement professionnel. En effet, au domicile d'un particulier, comme cela a été expliqué précédemment[384], il est plus aisé de saisir et de mettre les ordinateurs sous scellés afin de les analyser ultérieurement.

253. Une puissance d'investigation parfaitement adaptée aux environnements complexes. – Il en va tout autrement avec la complexité du système d'information d'une structure professionnelle, au sein de laquelle l'association des dispositions de l'article 57-1 et de l'article 56 offre de larges et puissantes possibilités d'investigations numériques que l'on peut qualifier de « perquisition informatique » *(A)*, mais pour

[381] C. pr. pén. art. 94.
[382] Crim. 6 nov. 2013, n°12-87.130 : JurisData n°2013-024912.
CHAVENT-LECLÈRE Anne-Sophie, *Affaiblissement de la distinction entre réquisition afin d'obtenir des documents et réquisition afin d'obtenir des informations,* LexisNexis, Procédures n° 2, Février 2014, comm. 56.
[383] Cette notion renvoi à l'art.41 du C. de pr. pén. : « Le procureur de la République procède ou fait procéder à tous les actes nécessaires à la recherche et à la poursuite des infractions à la loi pénale. ».
[384] V. *supra* n°249.

lesquelles le risque d'extraterritorialité des données soulève d'importantes incertitudes *(B)*.

A. La puissance des dispositions de la « perquisition informatique »

254. Une puissance insuffisamment encadrée. – L'association des mesures autorisant la « perquisition informatique » offre une puissance d'investigation et une latitude aux enquêteurs *(1)* telles, qu'il est regrettable que les actes correspondants ne soient pas mieux encadrés *(2)*.

1. Une puissance certaine

255. Une parfaite imbrication des différentes dispositions. – Le schéma de l'illustration n°1 (en page suivante) montre l'enchaînement des différentes dispositions ainsi que leurs effets sur la récupération de données lorsqu'elles sont actionnées, tout particulièrement en termes d'efficacité. En matière numérique, la loi s'est parfaitement bien adaptée à la réalité de la dématérialisation des informations[385] et de la montée en puissance des hébergements de type *cloud* [386], puisqu'elle permet de perquisitionner un système d'information distant[387] dès lors que les données sont accessibles depuis ce lieu.

256. La fouille des données physiquement présentes sur le lieu de la perquisition *(a)* est distinguée de la fouille des données géographiquement distantes *(b)*.

…/…

[385] Sur la relation entre données et informations, v. *supra* n°6.
[386] V. *supra* n°221.
[387] C'est-à-dire que les données ne sont pas physiquement dans le lieu où se trouvent les enquêteurs.

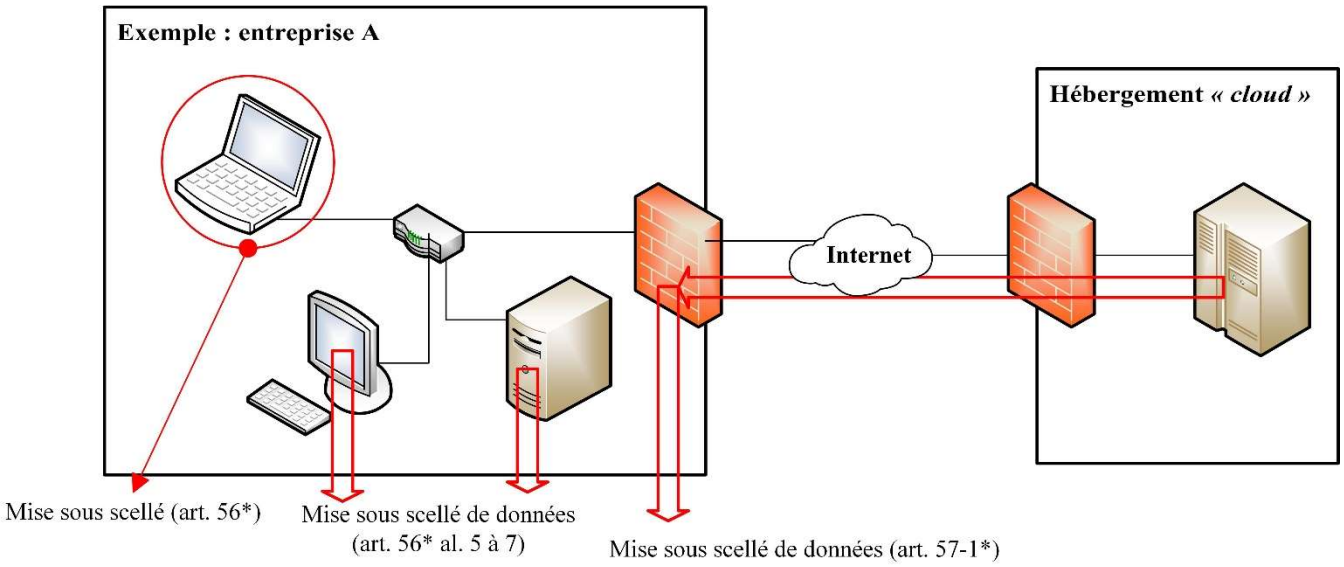


Illustration n°1 : investigations numériques dans le cadre des perquisitions

a. La fouille des données locales

257. Les investigations sur les données locales. – Grâce à l'article 56, les enquêteurs peuvent exploiter[388] puis, le cas-échéant, copier et saisir les données présentes. Il peut s'agir, par exemple, de données enregistrées sur le disque dur de la station de travail d'un salarié, ou des données stockées sur les serveurs physiquement présents dans les locaux de l'établissement perquisitionné. Hormis dans des cas extrêmes, et contrairement à ce qui a été dit pour le domicile d'un particulier[389], il est plus délicat, dans une entreprise, de placer sous main de justice un ordinateur complet, surtout s'il s'agit d'un serveur indispensable au fonctionnement de la structure.

258. La forte limitation technique de l'accès aux données locales. – Avec la dématérialisation de plus en plus importante due à la généralisation du *cloud*[390] la recherche d'éléments sur les différents supports digitaux physiquement présents dans les locaux d'une entreprise trouve rapidement ses limites. C'est le cas, notamment, lorsqu'un groupe de sociétés est composé de plusieurs filiales ou même de plusieurs sites, au sein duquel les serveurs sont mutualisés et centralisés sur un site unique. Le plus souvent, ce

[388] C'est-à-dire procéder à des constatations en décrivant dans le procès-verbal de perquisition des informations découvertes sous forme numérique.
[389] V. *supra* n°252.
[390] V. *supra* n°221.

site unique est géographiquement distant et les données centralisées sont accessibles au travers d'un réseau de communication électronique[391]. Tous les *cloud* privés[392] sont dans ce cas. En effet, un *cloud* privé repose sur une infrastructure informatique à haute disponibilité et généralement virtualisée, mais qui n'est accessible que depuis un intranet[393], contrairement au *cloud* public qui est accessible depuis n'importe quel ordinateur connecté à Internet (ce qui n'exclue bien évidemment pas une gestion de l'authentification et des mesures de sécurité pour l'accès aux données). Une illustration typique du *cloud* public est l'hébergement de données et d'applications[394] chez un prestataire de service (comptabilité, progiciel de gestion de la relation client, etc).

259. Conclusion du sous-paragraphe a : la fouille des données locales. – Face à de telles limitations dues à l'évolution des environnements informatiques et à la généralisation de l'hébergement délocalisé des informations numériques, des dispositions spécifiques prennent le relais pour autoriser les autorités judiciaires à accéder à ces informations distantes.

b. La fouille des données distantes

260. Les investigations sur des données distantes. – Les dispositions de l'article 57-1 permettent aux enquêteurs procédant à la perquisition, de pouvoir réaliser des investigations sur ces données, pourtant physiquement non présentes dans les locaux objets de la perquisition. Le prérequis est que les données cibles soient accessibles depuis l'un des postes présents sur les lieux où se déroule la perquisition. Or, cette condition sera vérifiée quasiment tout le temps dans le contexte technique qui vient d'être décrit, puisque les salariés d'une entreprise ou d'un site ont nécessairement un accès aux informations numériques qui sont le support de leur activité professionnelle.

261. Une large souplesse d'investigation sur les données distantes. – Les possibilités offertes par l'article 57-1 dépassent l'autorisation d'accéder à des données distantes

[391] Tel que défini dans le Code des postes et des communications électroniques, art. L32 2°) – V. *infra* n°539.
[392] Pour une définition du cloud privé, v. TOTEL Jérôme, *Multicloud : les questions à se poser avant de définir sa stratégie,* Silicon, 28 mars 2019 : « cloud privé : hébergés dans des datacenters privés ou en colocation. »
[393] Il s'agit d'un réseau privé permettant de relier les sites via des liaisons dédiées, ou au travers d'Internet en s'appuyant sur des liaisons de type VPN permettant la transmission des données dans un tunnel crypté.
[394] Le plus souvent il s'agira de logiciels fonctionnant en mode SAAS : v. *supra* n°221.

depuis le site où se déroule la perquisition. En effet, les enquêteurs peuvent également procéder à ces investigations numériques depuis « […] un système d'information implanté dans les locaux d'un service ou d'une unité de police ou de gendarmerie […] », dès lors que les données sont accessibles depuis le site perquisitionné[395]. Cette disposition présente un intérêt pratique important. Elle offre la possibilité aux enquêteurs de disposer d'outils d'investigations numériques plus puissants que ceux qui peuvent être déplacés sur les lieux de la perquisition, pour procéder à des recherches performantes sur les informations distantes susceptibles d'intéresser les faits.

262. Une limitation majeure à la souplesse du lieu déporté pour accéder aux données distantes. – Toutefois, cette possibilité de procéder à des investigations sur des données distantes depuis une Gendarmerie ou un Hôtel de police se heurte à la règle qui veut que toute perquisition se déroule en présence du suspect, ou de témoins[396] (suivant le stade et les conditions de la perquisition). Ainsi, la seule hypothèse où ces investigations déportées deviennent réellement possibles, serait le cas où une perquisition se prolonge par la garde à vue d'un individu. Il serait alors aisé que les investigations à distance se déroulent en sa présence, dans les locaux des officiers de police judiciaire.

263. Conclusion du sous-paragraphe 1 : une puissance certaine. – Les dispositions relatives à la perquisition se sont bien adaptées à la dématérialisation des informations et l'hébergement de type *Cloud*[397]. L'imbrication des articles 56 et 57-1 du Code de procédure pénale offre une véritable puissance d'investigation aux autorités judiciaires. D'ailleurs, il est regrettable que cette puissance ne soit pas mieux encadrée.

---

[395] QUEMENER Myriam et DALLE Frédérique, *L'accès à la preuve numérique, enjeu majeur de toute enquête pénale : pratique et perspectives*, Dalloz IP/IT, 2018, p.418.

[396] Crim. 3 avr. 2007 n°07-80.807 : JurisData n°2007-038632.
Sur la présence d'un tiers lors de la perquisition, v. *infra* n°325.

[397] L'article 57-1 autorisant l'accès à des données distantes date de 2003 : loi n°2003-239 du 18 mars 2003 pour la sécurité intérieure, art. 13.
CUTAJAR Chantal, *La loi pour la sécurité intérieure (principales dispositions)*, Recueil Dalloz 2003 p.1106.

2. Un encadrement insuffisant.

264. Les limitations de la perquisition « classique ». – Les seules limitations qui s'imposent aux investigations numériques diligentées lors d'une perquisition sont celles prévues pour les perquisitions en général. Il s'agit donc essentiellement de l'encadrement strict qui est prévu pour certaines professions[398].

265. Une absence de limitation regrettable. – Il est regrettable que la puissance de la perquisition informatique à distance n'ait pas fait l'objet d'un meilleur encadrement pour équilibrer l'efficacité de la mesure avec la protection des libertés individuelles, dont, tout particulièrement, le respect de la vie privée[399]. En effet, le fonctionnement usuel d'un système d'information fait que l'accès à une application ou à un espace de stockage hébergé en mode *cloud*, est possible moyennant des droits d'accès. Ceux-ci sont le plus souvent fonction des qualités et de l'emploi de l'utilisateur sur le système distant.

266. Par exemple, en entreprise, le service des ressources humaines n'a pas accès aux mêmes données que la comptabilité ou le service commercial. Il en est de même dans le cadre d'une utilisation familiale où une session[400] distincte peut être créée par chacun des membres de la famille. Or, fréquemment, la perquisition cible uniquement une ou quelques personnes précises. Il serait donc légitime que l'accès distant offert aux enquêteurs en vertu de l'article 57-1 du Code de procédure pénale, ait été limité aux données auxquelles la personne suspectée a accès lorsqu'elle a été identifiée sur le système informatique. En l'état, ce n'est pas le cas puisque l'article 57-1 laisse un accès total aux données du site distant dès lors qu'elles « sont accessibles à partir du système initial ou disponibles pour le système initial ». La notion de « système initial » n'apporte aucun encadrement des données accessibles.

267. Ce sont donc toutes les informations numériques présentes dans le système distant que les enquêteurs peuvent perquisitionner, y compris des données techniques[401], même si la personne visée par la mesure n'occupait, par exemple, que des fonctions de

[398] C. pr. pén. art. 56-1 pour les avocats, art. 56-2 pour la presse, etc.
PY Bruno, *Secret professionnel – Opposition du secret*, Dalloz Répertoire de droit pénal et de procédure pénale, Février 2017.
[399] Sur la protection des libertés individuelles, v. *infra* n°313.
[400] Au sens informatique du terme : sur un même ordinateur, même familial, il est possible de créer plusieurs comptes utilisateurs.
[401] Journaux de connexion, d'ouverture de session, fichiers de configuration, etc. Ces fichiers contiennent nécessairement des informations personnelles relatives à d'autres personnes que celle visée par la mesure.

secrétariat. Dans cet exemple, elle n'a, en aucun cas, accès à ces données techniques dans le cadre des missions qu'elle exerce.

268. Conclusion du sous-paragraphe A : la puissance des dispositions de la « perquisition informatique ». – La « perquisition informatique » fait référence aux dispositions spécifiquement prévues pour les données, au sein de la perquisition. La fouille des données ainsi autorisées aux autorités judiciaires offre une puissance d'investigation importante, qui mériterait d'être mieux encadrée quant aux informations numériques auxquelles les enquêteurs procédant à la mesure sont susceptibles d'accéder.

269. De plus, dès la création de l'article 57-1 par la loi du 18 mars 2003[402], le législateur a explicité l'autorisation d'accéder à des données situées en dehors du territoire national, ce qui soulève plusieurs incertitudes.

B. Les incertitudes autour de l'extraterritorialité des données

270. Un cadre légal et une vision technique qui s'opposent. – Les données hébergées à des milliers de kilomètres sont totalement identiques, d'un point de vue informatique, à celles qui sont sur le disque dur de l'ordinateur de bureau. *A contrario*, le cadre légal de la perquisition en ligne maintient une distinction pour les données hébergées à l'extérieur de nos frontières.

Il est donc nécessaire de préciser le cadre juridique applicable en matière d'extraterritorialité des données *(1)* pour constater les difficultés que celui-ci soulève *(2)*.

1. Le cadre juridique des données hébergées à l'étranger

271. Un cadre juridique protéiforme. – Le troisième alinéa de l'article 57-1 dispose que « s'il est préalablement avéré que ces données […] sont stockées dans un autre système informatique situé en dehors du territoire national, elles sont recueillies par l'officier de police judicaire, sous réserve des conditions d'accès prévues par les engagements internationaux en vigueur ». Dès lors, plusieurs cas sont à distinguer.

272. En Europe. – En matière d'engagements internationaux, la Convention de Budapest sur la cybercriminalité du 23 novembre 2001[403] est en lien avec la notion

[402] Loi n°2003-239 du 18 mars 2003 pour la sécurité intérieure.
[403] Cette convention a fait l'objet, le 28 janvier 2003, d'un protocole additionnel, relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques.

d'extraterritorialité[404]. Or, cette convention est applicable dans tous les états membres du Conseil de l'Europe, dont la France, ainsi que quelques autres états l'ayant ratifiée[405]. L'article 32 de ladite convention définit les « accès transfrontière à des données stockées, avec consentement ou lorsqu'elles sont accessibles au public », dans deux hypothèses. Dans la première, si « les données informatiques stockées sont accessibles au public (source ouverte) » alors leur accès est possible sans autorisation du pays où se situe l'hébergement. Ce cas de figure ne peut pas correspondre à la réalité des environnements qui viennent d'être décrits, puisque les hébergements de données professionnelles supposent, *a minima*, des accès soumis à une identification, qui s'opposent clairement aux notions de « source ouverte » et « d'accessible au public » posées par l'article 32.

273. Une autorisation préalable. – Avec la seconde hypothèse, il faut obtenir « le consentement légal et volontaire de la personne légalement autorisée à […] divulguer ces données […] ». Ainsi, toutes les structures multi-sites ayant optées pour un hébergement centralisé au travers d'un intranet[406] tombent sous le coup de cette obligation. Or, le rapport explicatif à la convention de Budapest sur la cybercriminalité[407] soulève précisément, au sujet de l'article 32, que « la question est de savoir qui est la personne "légalement autorisée" ». Un début de réponse est apporté en désignant, outre la personne à l'origine du dépôt, les personnes ayant une autorité légale. Avec l'exemple d'un groupe d'entreprise multi-sites, cela suppose obtenir l'accord du représentant légal de la structure distante.

274. Les conventions d'entraide pénale. – Il existe beaucoup de conventions d'entraide pénale signées par la France[408]. Néanmoins, celles-ci ne sont pas aussi détaillées que la convention de Budapest avec la notion de données ouvertes ou privées,

---

[404] Cette convention, bien qu'ancienne, est encore un texte sur lequel la doctrine continue de s'appuyer v. MONTEIL Marine, *L'usurpation d'identité à l'épreuve du numérique*, Recueil Dalloz 2020 p.101.
[405] Afrique du Sud, Canada, Etats-Unis d'Amérique, Japon.
[406] Voir *supra* n°258.
[407] Rapport explicatif de la Convention de Budapest sur la cybercriminalité du 23 novembre 2001. Source : www.europea.eu.
[408] V. par ex. : Convention d'entraide judiciaire en matière pénale entre la France et l'Afrique du Sud du 31 mai 2001.
Le traité d'entraide judiciaire en matière pénale signé le 10 décembre 1998 entre la France et les Etats-Unis d'Amérique et le décret n° 2010-489 du 12 mai 2010 portant publication de l'instrument relatif à l'application du traité d'entraide judiciaire en matière pénale signé le 10 décembre 1998 entre la France et les Etats-Unis d'Amérique, signé à La Haye le 30 septembre 2004.
US-EU MLAT : accord entre l'Union européenne et les États-Unis d'Amérique en matière d'entraide judiciaire du 19 juillet 2003.

et celle de la personne légalement autorisée à permettre l'accès aux informations numériques lui appartenant. Ces conventions définissent principalement le circuit des demandes et les modalités de transmission des informations.

275. L'absence d'engagement international. – Lorsqu'il n'existe pas de convention d'entraide pénale avec le pays où sont hébergées les données auxquelles les enquêteurs doivent accéder pour mener à bien la perquisition informatique, ce sont les dispositions générales qui sont applicables[409]. Dans ce cas, la demande d'entraide doit transiter par le ministère de la justice français qui prend à sa charge la saisine des autorités judiciaires étrangères. Une procédure d'urgence est prévue pour que les autorités judiciaires françaises puissent directement saisir leurs homologues étrangères, mais cette procédure reste très théorique car rien n'oblige les autorités judiciaires d'un pays avec lequel il n'y a aucun accord à aider spontanément la justice française en dehors de toute voie diplomatique.

276. Conclusion du sous-paragraphe 1 : le cadre juridique des données hébergées à l'étranger. – Lorsqu'une perquisition informatique conduit les enquêteurs à accéder à des données hébergées en dehors du territoire national, le régime commun qui se dégage est de devoir obtenir une autorisation. Dans le cas d'un pays signataire de la convention de Budapest, l'autorisation d'une personne ayant autorité sur les informations numériques concernées suffit, tandis que dans les autres cas c'est un circuit par voie diplomatique qui est nécessaire.

La nécessité d'obtenir une telle autorisation, quelle que soit la forme qu'elle prenne, soulève des difficultés.

[409] C. pr. pén. art. 694 et s.
BEAUVALLET Olivier, *Entraide judiciaire internationale – Dispositions générales*, JurisClasseur Procédure pénale Fasc. 20, 2018 : « Il s'agit ainsi de rechercher, dans la répression de la délinquance transfrontalière mais plus généralement dans le contexte d'une très grande circulation des personnes et des biens, une plus grande efficacité des investigations. »

2. Les difficultés du cadre juridique de l'extraterritorialité des données

277. Une double difficulté. – Le cadre légal de l'extraterritorialité des données lors d'une perquisition informatique soulève une première difficulté intuitivement évidente quant à la compatibilité du délai pour obtenir les autorisations théoriquement nécessaires avec le temps d'une perquisition *(a)*, puis une seconde qui provient des ambiguïtés ouvertes par la formulation de l'article 57-1 *(b)*.

a. La difficulté du délai pour obtenir une autorisation

278. L'incompatibilité des procédures d'entraide avec le temps d'exécution d'une perquisition. – Quel que soit le régime applicable[410], le temps pour obtenir l'autorisation nécessaire à l'accès aux données hébergées dans un pays étranger est clairement incompatible avec les délais d'exécution d'une perquisition. Pour que la coopération internationale puisse fonctionner, il faudrait que les demandes correspondantes aient été anticipées en amont de la perquisition. Or, la difficulté réside dans le fait que les enquêteurs ne savent pas, en avance, où sont hébergées l'ensemble des données auxquelles ils sont susceptibles d'accéder lors de la perquisition.

279. L'incertitude autour de la localisation des données. – Hormis dans le cas de groupes internationaux où les enquêteurs appelés à procéder à une perquisition au sein d'une unité de ce groupe, peuvent légitimement supposer préalablement à l'intervention qu'ils risquent de se trouver dans cette situation[411], rien, dans la majorité des autres perquisitions, ne peut permettre aux officiers de police judiciaire d'imaginer ce type de configuration en amont. En effet, la facilité et l'accessibilité en termes de tarifs aux hébergements de type *cloud*[412] peuvent placer les enquêteurs face à cette difficulté, alors même que la perquisition a lieu dans des structures ne disposant pas d'entité à l'étranger, voire même chez des particuliers. Avec la généralisation du *cloud*, il en ressort une

[410] Régime de la convention de Budapest, convention d'entraide internationale, régime général prévu à l'article 694 du C. de pr. pén.
SAINT-PAU Jean-Christophe, *Loi Perben II - L'entraide judiciaire internationale et européenne*, LexisNexis Droit pénal n° 7/8, Juillet 2004, étude 9 : « Le principe de souveraineté nationale permet ainsi à chaque État d'opérer un contrôle des demandes avant la transmission à l'autorité judiciaire. Nuisant à la rapidité et ainsi à l'efficacité de la procédure, ce contrôle politique n'est pas toujours nécessaire. »
[411] Les grands groupes d'entreprises réparties dans plusieurs pays centralisent le plus souvent l'hébergement de leurs données. L'hébergement centralisé peut ne pas être en France.
[412] V. *supra* n°221.

importante incertitude sur la localisation des données perquisitionnées[413]. Les enquêteurs peuvent même procéder à la mesure sans se rendre compte qu'ils accèdent à des informations hébergées à l'extérieur des frontières nationales.

280. Conclusion du sous-paragraphe a : la difficulté du délai pour obtenir une autorisation. – Le régime applicable en matière d'extraterritorialité des données auxquelles les enquêteurs doivent accéder lors d'une perquisition informatique importe peu car la difficulté réside précisément dans le moment où la localisation des informations numériques est constatée. En effet, dès l'instant où l'extraterritorialité est découverte lors de la perquisition, les délais pour obtenir les autorisations nécessaires ne sont pas compatibles avec le déroulement d'une perquisition.

281. Cette première difficulté est accentuée par une deuxième qui découle directement de la lettre de l'article 57-1.

b. La difficulté introduite par l'article 57-1

282. L'incertitude autour du régime applicable. – La condition introduite par l'article 57-1 du Code de procédure pénale au sujet de l'extraterritorialité des données emploie une formulation ambigüe : « s'il est préalablement avéré que ces données […] sont stockées […] en dehors du territoire national […] ». Une incertitude se dégage des mots « préalablement avéré ». En effet, il semblerait que les régimes d'autorisation qui viennent d'être évoqués ne s'appliquent pas tout le temps. Si les enquêteurs ne savent pas que les données sont localisées à l'extérieur des frontières nationale, un régime dérogatoire exempterait les autorités judiciaires de respecter « les conditions d'accès prévues par les engagements internationaux en vigueur ».

283. Une jurisprudence contestable. – L'arrêt de la Cour de cassation du 6 novembre 2013 déjà cité[414] semble aller dans ce sens en indiquant « qu'en l'absence de preuve que les données recherchées étaient stockées sur le territoire des Etats-Unis », rien « ne justifiait la mise en œuvre d'une procédure d'entraide pénale ».

[413] Sur l'importance de l'hébergement externalisé, v. BOURHA Nadia, *SaaS, PaaS, IaaS... que choisir?* Direction informatique, 28 octobre 2013.
[414] *Op. cit.* p.35 Crim. 6 nov. 2013, n°12-87.130 : JurisData n°2013-024912.

284. Cette interprétation soulève toutefois de nombreuses incertitudes[415]. En premier lieu, il convient de rappeler que le principe de licéité des preuves s'applique strictement aux autorités judiciaires[416]. Tout d'abord, il paraît sage de considérer que la présomption « d'ignorance » des enquêteurs sur l'hébergement à l'étranger des informations numériques est une présomption simple. Ensuite, ce raisonnement soulève la question de la charge de la preuve visant à démontrer l'extraterritorialité des données saisies. Si une information judiciaire est ouverte, le défendeur pourra soulever ce point et demander au juge d'instruction de procéder à toutes les mesures utiles permettant de vérifier le lieu où étaient hébergées les données saisies.

285. En second lieu, s'il ressort des résultats de ces diligences que les serveurs perquisitionnés étaient à l'étranger, la nullité des données saisies pourra être invoquée. Sur ce point, la Cour de cassation a déjà affirmé avec fermeté son exigence que des données obtenues dans un pays étranger au travers d'une investigation numérique respecte les procédures internationales en vigueur[417].

286. Une complexité difficile à traiter sans information judiciaire. – L'application du régime dérogatoire qui dispenserait les enquêteurs de respecter les conditions d'accès prévues par les engagements internationaux est d'autant plus contestable qu'elle introduit une différence notable dans l'exercice des droits de la défense suivant qu'une information judiciaire a été ouverte ou pas. En effet, si le dossier reste au stade de l'enquête préliminaire et que le prévenu est directement renvoyé devant le tribunal correctionnel, le réel exercice des droits de la défense face à une question aussi pointue devient beaucoup plus sensible. Alors que l'information judiciaire prévoit des accès réguliers au dossier d'instruction pour la personne mise en examen[418], un prévenu qui est directement renvoyé devant le tribunal correctionnel découvre les charges retenues contre lui et les preuves correspondantes, en fin de procédure. Ainsi, même s'il peut invoquer des nullités devant

[415] HENNION-JACQUET Patricia, *Précisions sur la régularité des actes d'enquête (citius, altius, fortius : oui, mais sans dopage)*, Recueil Dalloz 2013 p.2826 : « Cette solution semble toutefois critiquable. Si le site visité par les enquêteurs est bien ouvert au public, il n'en reste pas moins que l'espace auquel ils ont accédé était personnel et qu'ils y ont pénétré sans assentiment. […] »
[416] V. *supra* n°132.
[417] Crim. 10 Avril 2018 n°17-85.607 : JurisData n°2018-005644. Crim. 9 fev. 2016 n°15-85.071.
[418] C. pr. pén. art. 144. L'accès au dossier est prévu préalablement à chaque interrogatoire pour un mis en examen. Ainsi, si une perquisition informatique a eu lieu avant un interrogatoire, la défense aura accès aux procès-verbaux correspondants et pourra éventuellement s'interroger sur la localisation des données auxquelles les enquêteurs ont accédé.

le tribunal correctionnel[419], *in limine litis*, sa défense a moins le temps d'analyser les éléments du dossier que lors de l'information judiciaire où l'accès au dossier se fait régulièrement. Un doute sur la localisation des données auxquelles auraient accédé des enquêteurs lors d'une perquisition, nécessite une analyse hautement technique du dossier. Le renvoi direct vers le tribunal correctionnel laisse donc moins de possibilité à la défense de détecter une anomalie sur une éventuelle extraterritorialité des données qui n'aurait pas été régulièrement traitée par les enquêteurs, que lorsqu'une information judiciaire est ouverte.

287. L'inutilité du nouvel article 802-2 face à l'amoindrissement des droits de la défense en matière de perquisition informatique. – La loi du 23 mars 2019[420] a créé la possibilité d'invoquer la nullité d'une perquisition durant l'enquête[421], en précisant que dans « le cadre des recours examinés […], le requérant ne peut prétendre qu'à la mise à disposition des seules pièces de la procédure se rapportant à la perquisition qu'il conteste ». Dès lors, une personne ayant fait l'objet d'une perquisition pourrait, par ce biais-là, obtenir une copie des documents relatifs à la perquisition et, ainsi, disposer de plus de temps pour étudier, notamment, si la localisation des données par les enquêteurs a correctement été traitée. Néanmoins, le législateur a réservé cette procédure d'annulation aux seules personnes ayant été perquisitionnées, mais n'ayant pas fait l'objet de poursuites dans les « six mois après l'accomplissement de l'acte[422] ». Cette limitation neutralise l'égalité vers laquelle aurait pu tendre l'enquête et l'information judiciaire sur la capacité d'un prévenu à étudier la bonne application des dispositions en matière d'extraterritorialité des données fouillées lors d'une perquisition.

288. Conclusion du sous-paragraphe 2 : les difficultés du cadre juridique de l'extraterritorialité des données. – La formulation de l'article 57-1, confirmée par la jurisprudence, laisse subsister une incertitude dangereuse pour la stabilité des procédures.

---

[419] Sur le régime des nullités, dont la différence entre l'information judiciaire et la juridiction de jugement, v. *infra* n°857.

[420] Loi n°2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice. *Op. cit.* p.18.

[421] C. pr. pén. art. 802-2, créé par la loi du 23 mars 2019.

[422] C. pr. pén. art. 802-2 al. 1er : « Toute personne ayant fait l'objet d'une perquisition ou d'une visite domiciliaire en application des dispositions du présent code et qui n'a pas été poursuivie devant une juridiction d'instruction ou de jugement au plus tôt six mois après l'accomplissement de cet acte peut, dans un délai d'un an à compter de la date à laquelle elle a eu connaissance de cette mesure, saisir le juge des libertés et de la détention d'une demande tendant à son annulation. »

Ce flou doit être levé car la cybercriminalité implante volontairement ses serveurs dans des pays protecteurs pour leurs activités[423]. Il serait dommageable que des preuves numériques déterminantes dans un dossier soient annulées en raison de ce flou. Soit le législateur doit préciser qu'il incombe aux enquêteurs de vérifier où se situe le système d'information distant auquel ils accèdent. Si celui-ci est situé hors de nos frontières, la fouille ou la collecte des données doit être stoppée le temps nécessaire pour obtenir les autorisations prévues en fonction du pays concerné. Soit c'est une solution plus cohérente avec la réalité technique qui est choisie, en considérant que, dès lors que les données sont accessibles depuis le système initial par la personne visée par la mesure, alors ces informations numériques peuvent être perquisitionnées.

289. Conclusion du paragraphe §1 : la perquisition. – Une véritable perquisition informatique est prévue au sein de la perquisition. Malgré un flou regrettable lorsque les données ciblées par la mesure sont localisées à l'étranger, cette perquisition offre une importante puissance d'investigation aux enquêteurs, leur permettant de fouiller des données, y compris situées sur un site géographiquement distant, de les extraire et de les copier.

290. De manière plus classique, la perquisition permet de saisir des objets contenant des données (ordinateur, téléphone, etc), de les placer sous scellés, afin que ces objets soient exploités ultérieurement, grâce à d'autres actes de fouille.

§2. Les autres actes de fouille de données

291. Des fouilles pas toujours explicitement évoquées. – La perquisition n'est pas le seul acte de procédure autorisant des fouilles : des actes concernent, par exemple, les bagages[424], les véhicules « sur réquisitions écrites du procureur de la république[425] », ou encore les navires et bateaux[426]. Il en est de même avec les informations numériques, au travers de mesures autorisant la fouille de certaines données.

Parmi ces mesures, il convient de distinguer celles qui font explicitement référence à la fouille des informations numériques *(I)* et celles qui ont un autre objet, mais qui permettent implicitement de telles investigations *(II)*.

[423] V. *supra* n°32.
[424] V. *supra* n°241.
[425] C. pr. pén. art. 78-2-2 : II.
[426] *Ibid.* : III.

I – Des fouilles explicitement prévues

292. Plusieurs actes pour la fouille explicite des données. – Tout d'abord, il convient de rappeler que la perquisition permet de saisir des objets contenant des données tels que des ordinateurs ou des téléphones. Les scellés ainsi obtenus doivent nécessairement, dans un second temps, être exploités aux fins d'y rechercher des éléments susceptibles d'intéresser la procédure en cours. Deux actes de procédures permettent de procéder à la fouille des scellés *(A)*.
Ensuite, un acte présent dans les procédures dérogatoires prévues pour la criminalité organisée permet la fouille des messageries numériques *(B)*.

A. La fouille des scellés numériques

293. Les suites de la saisie d'objets contenant des données. – Les perquisitions se traduisent le plus fréquemment par la saisie et la mise sous scellés de différents éléments, dont des supports numériques. Dès lors, des investigations doivent être diligentées sur ces objets pour fouiller les données qu'ils contiennent. Les différentes façons de procéder pour y parvenir s'inscrivent dans la procédure de droit commun puisque, quelle que soit l'infraction visée par le dossier, il est possible de faire appel à un expert en informatique[427]. Les enquêteurs peuvent également procéder directement à des investigations sur ces supports, même s'il existe des contraintes importantes pour eux.

294. L'analyse des supports numériques. – Dans le jargon professionnel, l'exploitation des supports numériques[428] s'appelle une analyse. On imagine aisément que ce terme a été, au départ, transposé depuis les analyses réalisées dans d'autres disciplines telles que la génétique ou la biologie.

295. Des supports aux différentes origines. – Les supports numériques susceptibles de nécessiter une exploitation au fin d'y rechercher tout élément en rapport avec les faits (ou, susceptibles de constituer une nouvelle infraction pénale[429]) peuvent avoir plusieurs

[427] Dans le cadre de la réquisition à expert, celle-ci n'est possible que pour les infractions passibles d'une peine d'emprisonnement (C. pr. pén. art. 67). Une telle mesure reste une procédure de droit commun car elle ne vise pas une liste d'infractions mais un seuil de gravité détaché des incriminations.
[428] Ordinateur, disque dur, carte mémoire, etc.
[429] Si tel est le cas, ces nouveaux faits peuvent venir compléter l'enquête en cours, donner lieu à l'ouverture d'une nouvelle enquête ou faire l'objet d'un réquisitoire supplétif (si l'exploitation des scellés a lieu au stade de l'instruction).

origines. Bien sûr, les scellés issus des opérations de perquisition, tel que cela a été décrit au paragraphe précédent, sont les plus nombreux dans la majorité des procédures.

296. Néanmoins, il peut également s'agir d'objets qui ont pu être saisis sur les lieux d'un crime flagrant puisque, dans ce cas, l'officier de police judiciaire, « sur les lieux du crime, veille à la conservation des indices et de tout ce qui peut servir à la manifestation de la vérité[430] ». Des ordinateurs ou autres supports numériques tombent évidemment sous le coup de cette disposition, différente de la perquisition dans ses effets sur les scellés.

297. Parmi les scellés à exploiter, on peut également trouver des supports numériques qui ont été envoyés en réponse à des réquisitions. En effet, l'article 60-1 du Code de procédure pénale dispose que les informations demandées peuvent être envoyées, « notamment sous forme numérique[431] ». Les enquêteurs exploitent le support, puis le placent sous scellés qu'ils référencent sur le procès-verbal décrivant l'exploitation.

298. Plus rarement, les victimes ou les témoins, lors de leurs auditions, peuvent spontanément remettre des objets aux autorités judiciaires[432], qui seront également placés sous scellés.

299. Les deux possibilités d'analyse des supports numériques. – La procédure pénale impose que l'ensemble des supports numériques susceptibles d'intéresser les faits soient mis sous scellés par les enquêteurs ou un magistrat[433], avant que leur analyse puisse être exécutée.

Celle-ci peut être confiée à un expert par le biais d'une ordonnance de commission d'expert ou une réquisition *(1)*. Il s'agit de la voie théoriquement usuelle.

Toutefois, la pratique n'est pas aussi simple puisqu'une exploitation des scellés par les enquêteurs eux-mêmes est fréquente *(2)*.

---

[430] C. pr. pén. art. 54.

[431] V. *infra* n°373.

[432] V. *supra* n°177.

Crim. 22 Mai 2002 n°01-86.184 : JurisData n°2002-015314. BUISSON Jacques, *La perquisition implique une recherche des indices,* LexisNexis Procédures n° 10, Octobre 2002, comm. 194.

La remise volontaire d'éléments n'entre pas dans le champ de la perquisition prévue à l'article 76 du C. pr. pén.

[433] Par exemple, un témoin ou la partie civile qui est auditionné par le juge d'instruction et qui vient à l'audition avec un ordinateur qu'il remet spontanément au juge.

1. L'exploitation des scellés par un expert.

300. Les deux saisines possibles des experts. – Le recours de moins en moins fréquent à l'information judiciaire avec, depuis de nombreuses années, une augmentation constante de l'alignement des prérogatives offertes en enquête avec celles du juge d'instruction, se retrouve dans les missions qui peuvent être confiées aux experts. En effet, en matière d'analyse de supports numériques, l'expertise qui peut être ordonnée à l'instruction *(a)* et la réquisition en enquête préliminaire ou de flagrance *(b),* se veulent désormais identiques dans leurs effets.

a. L'expertise

301. Le cadre légal et réglementaire des experts judiciaires. – Les règles relatives aux experts judiciaires sont prévues par la loi n°71-498 du 29 juin 1971[434] et le décret n°2004-1463 du 23 décembre 2004. Il existe également une importante jurisprudence sur ce qu'est une expertise et ce qui n'en est pas une[435]. Les experts judiciaires[436], dont les spécialités scientifiques sont très vastes, sont classés selon des rubriques définies par un arrêté du 10 juin 2005[437] et sont inscrits[438] sur des listes établies par les Cours d'appel, ou sur une liste nationale pour les experts près la Cour de cassation.

302. Des rubriques inadaptées à la procédure pénale. – En procédure pénale, ces rubriques conviennent pour toutes les disciplines telles que la médecine ou la biologie (les rubriques « F »). Le juge pénal trouve aisément ce qu'il cherche. En revanche, la nomenclature pose des difficultés dans l'ensemble des disciplines techniques des rubriques « E », comme la mécanique, hydraulique, ou encore, bien sûr, l'informatique. En effet, dans ces disciplines, la majorité des expertises sont ordonnées en matière civile ou commerciale[439], ce qui se ressent dans la nomenclature. Deux rubriques concernent l'informatique au sens large : E1, « électronique et informatique », et G2.5 « investigations scientifiques et techniques – documents informatiques ».

---

[434] Modifiée par la loi n°2004-130 du 11 février 2004.
[435] PRADEL Jean et VARINARD André, *Les grands arrêts de la procédure pénale,* 8ème édition, Dalloz : p.248 et s.
[436] BOULEZ Jacques, *Expertises judiciaires – Désignation et mission de l'expert – Procédure selon la juridiction,* DELMAS, 13ème édition.
RUELLAN François et MARIE Nathalie, *Droit et pratique de l'expertise judiciaire civile,* LexisNexis.
[437] Arrêté du 10 juin 2005 relatif à la nomenclature prévue à l'article 1er du décret n°2004-1463 du 23 décembre 2004.
[438] SALATI Olivier, *Chapitre 123 – Inscription et réinscription sur les listes des cours d'appel – Personnes physiques et personnes morales,* Dalloz Droit de l'expertise, 2016.
[439] Contentieux liés à des dysfonctionnements, à des inexécutions ou des manquements contractuels.

303. Très clairement, seuls les experts de la rubrique G2.5 seraient censés être commis par des juridictions pénales, puisque sont regroupées dans le groupe « G » les sciences criminelles, tandis que la rubrique E1 est l'illustration de l'orientation « civile » de cette nomenclature, avec un mélange d'informatique, d'électronique et d'automatisme ce qui démontre la vision « industrielle » de cette catégorie et non « pénale ». Malheureusement, le déficit d'experts en informatique dans certaines Cours d'appel et le manque de clarté de cette classification pour les magistrats font que, souvent, sont commis des « experts en informatique », sans se préoccuper de la rubrique dans laquelle ils sont inscrits.

304. La mise en action d'une expertise. – D'un point de vue procédural, l'expertise est prévue au stade de l'instruction[440] par les articles 156 et suivants du Code de procédure pénale. L'expert est autorisé à briser les scellés pour procéder à l'étude technique de leur contenu[441], et ceci sans la présence de la personne mise en examen[442]. Au terme de sa mission, l'expert commis[443], reconstitue les scellés[444] et remet un rapport d'expertise à la juridiction d'instruction[445].

b. La réquisition

305. La transposition de l'expertise au stade de l'enquête. – Les réquisitions prévues à l'article 60 du Code de procédure pénale en enquête de flagrance et 77-1 en préliminaire peuvent également conduire, dans les faits, à l'intervention d'experts judiciaires[446.]

306. Une restriction effacée par la pratique. – Même si le texte continue de prévoir que la réquisition a pour objet « de procéder à des constatations ou à des examens techniques », la loi du 23 juin 1999[447] a modifié les deux articles en question en, d'une part, supprimant la condition de célérité qui était un prérequis indispensable jusque-là[448] et, d'autre part, en introduisant une sorte de diffusion du rapport « aux personnes à

[440] Et lors du jugement, mais cette possibilité est marginale et révèle le plus souvent une lacune dans la mise en état du dossier. C. pr. pén art. 156 : « Toute juridiction d'instruction ou de jugement […] peut […] ordonner une expertise. »
[441] C. pr. pén. art. 163.
DELBANO Fabrice, *Chapitre 332 – Pièces de procédure et Scellés,* Dalloz Droit de l'expertise, 2016.
[442] V. *infra* n°326.
[443] En matière d'investigations numériques, le principe est la commission d'un expert unique – la dualité est rarissime et le collège purement théorique.
[444] C. pr. pén. art. 166.
[445] *Ibid.*
[446] Le deuxième alinéa de l'article 60 fait explicitement allusion aux experts judiciaires au travers de la notion de prestation de serment.
[447] Loi n°99-515 du 23 juin 1999 renforçant l'efficacité de la procédure pénale.
[448] « […] qui ne peuvent être différées […] » a été supprimé.

l'encontre desquelles il existe des indices faisant présumer qu'elles ont commis ou tenté de commettre une infraction, ainsi qu'aux victimes ». Il s'agit là d'une ébauche de transposition des prérogatives des juridictions d'instruction[449].

307. De plus, la Cour de cassation a précisé lors d'un arrêt du 14 septembre 2005[450], que « l'article 77-1 du Code de procédure pénale confère au procureur de la république, agissant en enquête préliminaire, le pouvoir de charger toute personne qualifiée de missions techniques ou scientifiques de même nature que celles qui peuvent être confiées aux experts par le juge d'instruction en application de l'article 156 du même Code ». La chambre criminelle précise également que dès lors que « l'avis émis par le technicien reste soumis à la libre discussion des parties, selon les voies procédurales appropriées », les droits de la défense sont respectés.

308. Concrètement, il s'agit là d'un revirement de jurisprudence de la Cour de cassation[451] en ce qui concerne cette investigation numérique, puisqu'il est désormais suggéré que l'expert réquisitionné peut, par exemple, analyser dans le détail le contenu du disque dur d'un ordinateur, exactement comme il le ferait dans une expertise ordonnée par le juge d'instruction[452], ce qui a pour effet d'introduire, au stade de l'enquête, un acte d'investigation particulièrement puissant et intrusif[453].

309. Des garanties procédurales qui restent inégales. – Or, malgré l'introduction de la diffusion des « résultats des examens techniques et scientifiques », et malgré « la discussion selon les voies procédurales » évoquée par la Cour, ceci conduit à s'interroger sur le respect des droits de la défense, ainsi que du respect de la vie privée, consacré par l'article 8 de la Convention européenne des droits de l'homme. Tout d'abord, même si l'expertise pénale telle qu'elle est prévue à l'instruction n'est pas contradictoire dans son déroulé[454], plusieurs éléments ont été introduits pour l'améliorer dans ce sens,

---

[449] V. C. pr. pén. art. 167 qui encadre la diffusion du rapport ou des conclusions.

[450] Crim. 14 sept. 2005, n°05-84.021 ; Bull. crim. n°226, RSC 2006. 412, obs. J. Buisson.

[451] Crim. 29 sept. 1993 n°92-86.589 : JurisData n°1993-002565.
Crim. 21 mai 1997 n°95-84.050 : JurisData n°1997-003237.
La position de la chambre criminelle était ici inverse puisqu'elle a confirmé l'arrêt d'une Cour d'appel qui avait partiellement annulé un rapport réalisé au titre de l'art. 77-1 du C. pr. pén. au motif que celui-ci comportait « au-delà des constatations et examens techniques, des interprétations, des discussions et des appréciations qui ressortissent de l'expertise »..

[452] V. *supra* n°304.

[453] V. *infra* n°314.
MIANSONI Camille, *L'expertise pénale en enquête préliminaire et de flagrance. Le procureur de la République, prescripteur d'expertise*, AJ Pénal 2011 p.564.

[454] Les investigations se passent sans la présence des personnes concernées – V. *supra* n°304.

essentiellement en amont et en aval de celle-ci. Avant le début des opérations d'expertise, les parties peuvent demander des modifications sur la mission qui est confiée à l'expert[455].

310. Ensuite, au terme de la mission, l'article 167 encadre une diffusion parfaitement définie du rapport. Les parties peuvent alors demander des compléments ou une contre-expertise[456].

311. *A contrario*, au stade de l'enquête, le suspect n'a pas connaissance des éventuels éléments recueillis à charge[457]. Ainsi, le fait d'être informé beaucoup plus tardivement des résultats d'une expertise informatique diligentée sur des scellés numériques en enquête qu'à l'instruction est susceptible de nuire conjointement au respect des droits de la défense et de la vie privée[458].

312. En premier lieu, le droit à pouvoir se défendre équitablement, consacré à l'article 6 de la Convention européenne des droits de l'Homme, est fortement associé à la rapidité avec laquelle une personne est informée des preuves retenues contre elle[459].

313. En second lieu, dans un contexte de numérisation de notre société[460], les scellés numériques sont évidemment des supports forts de la vie privée d'une personne. En conséquence, le fait d'aligner les investigations réalisées au titre d'une réquisition sur celles de l'expertise, alors que cette dernière permet à la personne poursuivie de bénéficier de garanties plus fortes pour le respect de sa vie privée[461], constitue une intrusion allant à l'encontre de l'article 8 de la Convention européenne des droits de l'Homme. En effet, même si « une ingérence légale [dans la vie privée] est autorisée dès lors qu'elle vise la lutte contre les infractions pénales[462], » celle-ci doit se faire dans le respect d'un procès équitable. Le fait de n'avoir aucune information, ou tardivement, sur les recherches réalisées sur un support numérique, n'est pas compatible avec des investigations aussi avancées que celles autorisées au stade de l'instruction.

---

[455] C. pr. pén. art. 161-1.
[456] C. pr. pén. art. 167.
[457] En enquête préliminaire, par exemple, l'accès au dossier n'est possible que lorsque le prévenu est renvoyé devant le tribunal correctionnel. La chambre criminelle considère que les droits de la défense sont garantis, même si l'enquête est très longue : Crim. 3 mars 2015, n° 14-80.415 : JurisData n°2015-004059.
[458] AMBROISE-CASTEROT Coralie et COMBEAU Chantal, *La procédure pénale dans la balance : entre secret et transparence*, Dalloz, Les cahiers de la justice 2014, p.373.
[459] HENNION Patricia, *Preuve pénale et droits de l'Homme*, soutenue le 19 décembre 1998 à Nice-Sophia Antipolis, Septentrion, p.136
[460] V. *supra* n°17.
[461] Lors d'une expertise, la mission confiée à l'expert est communiquée aux parties : v. *supra* n°310.
[462] *Ibid*, HENNION Patricia, p. 190.

314. Des dispositions qui maintiennent une différence. – En effet, techniquement, il subsiste une différence importante entre procéder « à des constatations ou des examens » sur un support numérique et « l'expertiser ». Concrètement, le premier cas consiste, par exemple, à regarder dans le cadre d'une enquête pour agression sexuelle sur mineur, si l'ordinateur du suspect contient du surf sur des sites pédopornographiques. Autrement dit, il semble qu'une interprétation plus mesurée devrait retenir qu'il s'agit d'investigations ciblées, en rapport avec l'infraction à l'origine de l'enquête. Une expertise est une analyse complète du disque dur, ce qui sous-entend une intrusion particulièrement importante dans la vie privée du suspect, voire dans celle de sa famille[463]. Comme cela a été évoqué précédemment, une investigation aussi intrusive ne peut se concevoir que sous le contrôle d'un magistrat indépendant[464], ce qu'est le juge d'instruction et ce que n'est pas le procureur[465].

315. Une différence qui s'accentue en flagrance. – La réserve qu'il convient d'exprimer par rapport à l'alignement des réquisitions en enquête sur les expertises s'accentue davantage encore avec la procédure de flagrance. En effet, une partie de la doctrine considère que l'arrêt du 14 septembre 2005, visant l'article 77-1 du Code de procédure pénale s'applique automatiquement à l'article 60 relatif aux enquêtes de flagrance[466]. Cette position ne fait pas l'unanimité[467], car elle soulève des interrogations. L'objectif de l'enquête de flagrance reste avant tout de préserver les indices et tous les éléments nécessaires à la recherche des infractions et de leurs auteurs, à la différence des investigations touchant au fond de l'affaire lors de l'enquête préliminaire lui succédant ou de l'information judiciaire. D'ailleurs, l'arrêt du 14 septembre 2005 indique bien que c'est au procureur de la république qu'est conféré le pouvoir de confier aux experts le même type de mission qu'en instruction.

316. Or, la différence entre l'article 60 et 70-1 réside précisément dans le fait qu'en raison de la nécessité d'aller vite, l'officier de police judiciaire, en enquête de flagrance

---

[463] Cas d'un ordinateur familial : même si plusieurs comptes utilisateurs sont présents, l'expertise va analyser toutes les données, sans distinction.

[464] JOSSERAND Sylvie, *L'impartialité du magistrat en procédure pénale*, thèse soutenue en 1996 à Grenoble 2.

[465] MILOUDI Farouk, *Le procureur de la République et la procédure judiciaire*, thèse soutenue en 2010 à Nice.

[466] BUISSON Jacques, *Crimes et délits flagrants,* JurisClasseur Procédure pénale Fasc. 20, 156 : « […] un arrêt rendu relativement à l'article 77-1 du Code de procédure pénale, mais applicable mutatis mutandis à l'article 60 […] ».

[467] MIANSONI Camille, *L'expertise pénale en enquête préliminaire et de flagrance. Le procureur de la République, prescripteur d'expertise,* Dalloz AJ pénal 2011 p.564.

peut, seul, réquisitionner un expert, alors qu'en préliminaire c'est le procureur de la république qui est compétent (l'officier de police judiciaire en a la possibilité, mais uniquement sur autorisation du procureur)[468].

317. Comment, dans ce cas, une ingérence aussi forte que l'analyse d'un ordinateur telle qu'elle est réalisée lors d'une expertise pourrait être compatible, en enquête de flagrance, avec le respect des libertés individuelles ?

318. Une différence prolongée dans le document de synthèse. – Aux termes de sa mission, même si l'expert requis intitule le document qu'il remet « rapport[469] » comme lorsqu'il est commis pour une expertise en bonne et due forme, il est indispensable d'opérer une distinction entre ce « simple » rapport qui vient en réponse aux réquisitions et le rapport d'expertise. Pour employer des notions pédagogiques, le rapport d'expertise est un rapport tandis que le document restitué en cas de réquisition est censé être un compte-rendu, se limitant à décrire les constatations et les examens réalisés[470].

319. Conclusion du sous-paragraphe 1 : l'exploitation des scellés par un expert. – L'intervention des experts pour analyser des scellés contenant des données est la voie naturelle qui ressort de la procédure pénale. L'expertise sur des supports informatiques, ordonnée lors de l'information judiciaire est l'investigation numérique autorisant une analyse exhaustive des données contenues. La jurisprudence et l'assouplissement des contraintes légales, notamment par le biais de la suppression de tout critère d'urgence, tendent à aligner l'intervention des experts au stade de l'enquête avec l'expertise.

320. Les experts judiciaires ne sont pas les seules personnes susceptibles d'analyser les supports numériques.

---

[468] Sur la différence qui existe entre enquête de flagrance et préliminaire : v. CONTE Philippe, *Terrorisme - Bas les masques !* JurisClasseur, Droit pénal n°6, Juin 2016, repère 6.

[469] Crim. 17 sept. 2014 n°13-87.164 : « […] tendant à l'annulation de la réquisition du 30 novembre 2009 ainsi que du rapport d'expertise […]. »
Crim. 24 nov. 2015 n°14-87.689 : « […] que les analyses susvisées ont donné lieu à la rédaction de rapports détaillés ; »

[470] *Op. cit.* p. 35 MIANSONI Camille, *L'expertise pénale en enquête préliminaire et de flagrance. Le procureur de la République, prescripteur d'expertise,* Dalloz AJ pénal 2011 p.564 : « Au stade de l'enquête, les finalités immédiates de l'expertise pénale diffèrent de celles de l'expertise ordonnée par le juge[…]. »

2. L'exploitation des scellés par les enquêteurs

321. Des analyses de données réalisées par les enquêteurs. – Il existe des situations où les enquêteurs procèdent, par eux-mêmes, à des investigations sur des supports tels que des téléphones ou des ordinateurs saisis au cours de l'enquête. C'est notamment le cas lorsqu'une urgence existe et est incompatible avec la saisine d'un expert, qui suppose le respect d'un formalisme contraint[471].

322. Des règles et la réalité qui s'opposent. – Les possibilités d'intervention des enquêteurs pour procéder à des investigations sur des supports numériques sont fortement limitées par la procédure *(a)*.
Néanmoins, la réalité des dossiers en matière d'enquête, montre que les enquêteurs contournent souvent ces limitations pour que l'analyse des données précédemment saisies soit réalisée au sein d'un service de Police ou de Gendarmerie *(b)*.

a. Des possibilités d'analyses fortement limitées

323. L'organisation des services d'enquête en matière d'investigations numériques. – Les besoins de certaines enquêtes, notamment en terme de rapidité, poussent les enquêteurs à procéder par eux-mêmes à l'analyse de supports numériques saisis[472]. Cette situation n'est pas marginale puisque la Gendarmerie et la Police nationale ont répondu à ces besoins en créant des postes de spécialistes, voire des services spécialisés, en investigations numériques. Dans la Gendarmerie, les enquêteurs formés à cette fin sont les « N'Tech » et dans la Police ce sont les « ESCI[473] ».

324. Le cadre procédural d'intervention des enquêteurs spécialisés. – L'article 14 du Code de procédure pénale, qui définit les missions de la police judiciaire, précise qu'elle « est chargée […] de constater les infractions à la loi pénale, d'en rassembler les

[471] V. *supra* n°305. Le procureur (ou l'officier de police judiciaire en flagrance) doit réquisitionner un expert, lui transmettre les éléments, laisser un délai à l'expert, et se placer dans l'attente de la remise du rapport par celui-ci.
[472] V. les nombreuses et récurrentes communications de la Gendarmerie et de la Police sur leur capacité à exploiter des supports numériques : MICHEL Jean-Charles, *Les disques durs ne résistent pas à l'enquêteur*, Ouest France Morbihan, 12 mars 2012 – DUPRAT Florent, *Trente gendarmes formés pour enquêter sur le numérique,* La dépêche du Midi, 27 novembre 2018 : « […] Extraire des données SMS d'un téléphone portable ou de courriels d'un ordinateur n'a plus vraiment de secrets pour eux. […] » - DUPONT Gilles, *Les escrocs du XXIe siècle sont à l'oeuvre sur la Toile,* Le Bien Public, 4 mars 2009 : « […] les ESCI […] analysent, décryptent, décodent, fouillent dans les historiques […]. »
[473] Enquêteur Spécialisé en Criminalité Informatique.

preuves et d'en rechercher les auteurs tant qu'une information n'est pas ouverte ». De plus, l'article D7 du même Code dispose que « les officiers de police judiciaire peuvent […] faire appel aux personnes qualifiées appartenant aux organismes spécialisés de la police nationale ou de la gendarmerie nationale », ce qui permet aux officiers de police judiciaire conduisant l'enquête, d'aller chercher une aide technique auprès de l'un de leur collègue spécialisé.

325. Les importantes limitations aux analyses par les enquêteurs. – En première lecture, l'article 14 offre une autonomie importante, ainsi que de larges possibilités d'investigations, aux enquêteurs. Néanmoins, cette apparente latitude se heurte rapidement à une restriction importante qui concerne tous les supports numériques ayant été saisis lors d'une perquisition, que celle-ci soit conduite en enquête ou à l'instruction.

326. En effet, lors des enquêtes de flagrance, l'article 56[474] dispose que « tous objets et documents saisis sont immédiatement inventoriés et placés sous scellés. Cependant, si leur inventaire sur place présente des difficultés, ils font l'objet de scellés fermés provisoires[475] jusqu'au moment de leur inventaire et de leur mise sous scellés définitifs et ce, en présence des personnes qui ont assisté à la perquisition suivant les modalités prévues à l'article 57 ». Dans le même temps, l'article 57 impose que la perquisition se déroule en présence de la « personne au domicile de laquelle la perquisition a lieu » ou en présence de deux témoins[476].

327. Lors de l'information judiciaire, les contraintes sont encore plus fortes puisque le sixième alinéa de l'article 97 dispose que « lorsque ces scellés sont fermés, ils ne peuvent être ouverts et les documents dépouillés qu'en présence de la personne mise en examen, assistée de son avocat, ou eux dûment appelés. Le tiers chez lequel la saisie a été faite est également invité à assister à cette opération ».

328. L'opposabilité des données soumise à une sorte de surveillance. – Il en ressort que tous les supports numériques saisis lors d'une perquisition, doivent être placés sous scellés en présence des personnes prévues par la loi[477] et ne sont donc susceptibles d'être

[474] En enquête préliminaire, moyennant le respect du principe du consentement obligatoire (outre les régimes dérogatoires prévus), l'art. 76 du C. pr. pén. indique que les dispositions de l'article 56 sont applicables, dont, forcément, celles relatives à la saisie.
[475] Sur le régime des scellés provisoires, v. *infra* n°334.
[476] C. pr. pén. art. 57, al 1 et 2.
[477] C. pr. pén. art. 57, 76 *(3ème alinéa)*, 95 et 96.

exploités qu'en leur présence, sauf dans le cas d'une expertise ou d'une réquisition à expert. Un régime dérogatoire à la présence de la personne mise en examen est explicitement prévu[478]. En effet, il pourrait être tentant d'affirmer que la présence de la personne à qui les données sont susceptibles d'être opposées n'est légalement imposée qu'au stade de l'information judiciaire. Cette interprétation va à l'encontre de l'esprit du texte. Pourquoi imposer la mise sous scellés d'un objet contenant des données en présence des personnes visées par la perquisition ou en présence de témoins, si c'est pour autoriser leur exploitation en leur absence ?

329. Ces règles imposant la mise sous scellés des objets en présence de tiers révèlent une sorte de suspicion ou, *a minima*, de défiance, à l'égard des enquêteurs. En effet, cette présence a pour objectif de couper court à toute contestation ultérieure d'une personne poursuivie ou mise en examen, qui mettrait en question la présence de l'objet saisie sur le lieu de la perquisition. Il s'agit de garantir une sorte « d'opposabilité pénale » des éléments saisis[479].

330. Le prolongement de la suspicion lors de l'analyse des données. – Il existe une différence majeure entre les données et les autres éléments saisis lors de la perquisition : leur immatérialité[480]. Dès lors qu'un objet, même infiniment petit, comme une trace ADN, a été mis sous scellé, il s'agit d'un élément matériel. Si son analyse venait à être contestée, une nouvelle analyse pourrait être ordonnée. L'exploitation des données est plus délicate. En raison de l'immatérialité des informations numériques, la mise sous scellés n'est pas une garantie suffisante. En effet, lors de l'exploitation du support, des données pourraient être introduites sans que cela ne laisse aucune trace.

331. De telles méthodes existent dans d'autres pays que la France. En Turquie, de nombreuses contestations sur la présence de données saisies au sein d'un objet retrouvé

[478] C. pr. pén. art. 163 al. 2 : « Pour l'application de leur mission, les experts sont habilités à procéder à l'ouverture ou à la réouverture des scellés, et à confectionner de nouveaux scellés après avoir, le cas échéant, procédé au reconditionnement des objets qu'ils étaient chargés d'examiner […] ; les dispositions du sixième alinéa de l'article 97 ne sont pas applicables. »

[479] Lorsque des irrégularités relatives à la mise sous scellés sont invoquées comme moyen de nullité, la chambre criminelle analyse systématiquement si ces irrégularités ont pu affecter l'intégrité des éléments mis sous scellés : v. par ex. Crim. 30 mars 2016 n°15-86.693, Bull. crim. 2016, n°110 : « Attendu qu'en cet état, et dès lors que, d'une part, il résulte de ces constatations que ce téléphone est toujours resté sous le contrôle de l'Inspection générale de la police nationale jusqu'à sa saisie par un fonctionnaire de ce service, de sorte qu'il n'existe aucun doute sur l'identité du téléphone saisi, d'autre part, les allégations du demandeur, selon lesquelles il aurait pu être porté atteinte à l'intégrité de son contenu avant le placement sous scellés sont, en l'absence de toute contestation sur les données extraites et transcrites dans les procès-verbaux, hypothétiques et, en conséquence, dépourvues de fondement […]. »

[480] V. *supra* n°219.

chez une personne poursuivie, a conduit à imposer que, désormais, toute saisie d'un support numérique doit s'accompagner du hachage[481] de ce support afin de pouvoir vérifier son intégrité *a posteriori*[482].

332. La nécessaire analyse des scellés en présence du tiers concerné. – La loi impose que les éléments saisis lors d'une perquisition le soient en présence de témoins afin d'écarter toute suspicion envers les enquêteurs sur la réelle présence de ces éléments sur le lieu visité. De plus, les données sont facilement modifiables. En conséquence, la présence du tiers aux analyses des données contenues dans un scellé s'impose.

333. L'exploitation concomitamment à une garde à vue. – Dans la pratique, les enquêteurs qui procèdent à la perquisition s'efforcent de ne jamais procéder eux-mêmes à l'exploitation des scellés contenant des données. Ils réquisitionnent un agent ou un militaire différent de celui qui a participé à la perquisition[483]. Les seules exceptions sont pratiquées dans un cadre précis, tenant à une souplesse permise par la procédure. Il est, en effet, fréquent que les enquêteurs procèdent à des investigations sur des supports[484] saisis lors d'une perquisition pendant la garde à vue d'un suspect.

334. Concrètement, les officiers de police judiciaire utilisent la mise sous scellés provisoires[485] pour transporter le support numérique jusqu'à leurs locaux. Au demeurant, dans le cas de données saisies lors d'une perquisition, la chambre criminelle a refusé d'annuler la saisie de ces données au seul motif que les enquêteurs n'avaient pas posé les scellés provisoires[486]. Ainsi, lorsque le suspect est placé en garde à vue à la suite de la perquisition [487], les enquêteurs[488] procèdent à l'analyse pendant cette durée et réalisent la mise définitive sous scellés telle qu'imposée par le texte dès qu'ils ont terminé. La

[481] FUHR Thomas, *Conception, Preuves et analyse de fonctions de hachage cryptographiques,* Thèse soutenue le 3 octobre 2011 : « Une fonction de hachage est un algorithme permettant de calculer une empreinte de taille fixe à partir d'une donnée de taille quelconque. »
[482] AKZOY RETONAZ Eylem, Maître de conférences à l'université de Galatasaray : entretien le 5 mai 2017 au Pôle juridique et judiciaire de Bordeaux. Madame AKZOY RETONAZ parle de « torture numérique avec des méthodes qui rappellent celles de l'inquisition. »
[483] V. *infra* n°350.
[484] Que ce soient des ordinateurs, des téléphones, etc.
[485] V. *supra* n°326.
[486] Crim. 14 oct. 2015 n°14-83.300, inédit : « […] la confection de scellés provisoires est une faculté laissée à l'appréciation des enquêteurs, agissant sous le contrôle du juge […]. »
[487] Ou dès le début de la perquisition comme l'impose la jurisprudence de la Cour de cassation lorsque la perquisition se déroule sous la contrainte pour le suspect.
[488] Ou leurs collègues spécialisés : les N'Tech ou les ESCI - voir *supra* n°323.

condition d'accomplir cette tâche « en présence de la personne ayant assisté à la perquisition » est alors aisée à vérifier puisque le protagoniste est en garde à vue.

335. Un régime plus souple pour les scellés non issus d'une perquisition. – Il convient de rappeler que ces limitations ne sont imposées que pour la perquisition et donc pour les saisies qui sont opérées dans ce cadre. Ainsi, tous les supports numériques non issus d'une perquisition[489] peuvent être analysés par les enquêteurs, sans qu'il y ait obligatoirement recours à un expert. Ces investigations font l'objet d'un procès-verbal[490], qui actera également la mise sous scellés de l'objet analysé, après son exploitation.

b. Le contournement des restrictions

336. Des limitations se heurtant aux besoins des enquêtes. – Souvent, les investigations sur les scellés saisis lors d'une perquisition, contenant des données, sont déterminantes pour la suite de l'enquête. C'est notamment le cas lorsqu'elles sont contenues dans un support saisi au domicile d'un suspect. Ainsi, les restrictions qui existent pour que les enquêteurs puissent procéder aux analyses correspondantes posent deux problèmes.

337. En premier lieu, dans des dossiers particulièrement sensibles comme en matière de terrorisme ou de grande criminalité, les officiers de police judiciaire doivent chercher des compétences et des moyens d'investigation dont ne peuvent pas disposer des experts indépendants *(α)*. En second lieu, dans le cas le plus courant, les enquêteurs ont besoin d'obtenir rapidement les résultats des investigations sur ces supports et essayent donc d'éviter de passer par une réquisition à expert, qui génère un délai d'exploitation nécessairement plus long *(β)*.

α. Un contournement pour utiliser la puissance d'investigation des services spécialisés

338. Des services à forte compétence. – Les N'Tech et les ESCI[491] ne sont pas les seuls spécialistes des investigations numériques au sein de la Gendarmerie et de la Police nationales. Ils sont en quelque sorte perçus comme des « experts internes » à la police et la gendarmerie, avec pour rôle de réaliser une assistance de proximité aux enquêteurs.

[489] V. *supra* n°296. et s.
[490] C. pr. pén., art. D9, D10 et D11.
[491] V. *supra* n°323.

De nombreux services tels que l'IRCGN[492], les différents laboratoires de la police scientifique, voire des services spécialisés en matière de répression du grand banditisme ou de lutte contre le terrorisme, disposent à la fois de matériel de pointe[493] et d'importantes compétences humaines[494] dans le domaine des investigations numériques.

339. En cas de criminalité organisée, de terrorisme mais, surtout, en cas de dossier fortement médiatisé, ce sont des services spécialisés qui sont saisis, et qui sont capables d'enquêter en autonomie, du moins pour ce qui concerne les investigations numériques. L'objectif recherché est, bien évidemment, la compétence et les moyens technologiques de ces services, dont ne peuvent disposer, ni les experts issus de la société civile, ni les N'Tech ou les ESCI. De plus, une interaction forte entre les officiers de police judiciaire et les militaires ou agents qui procèdent aux analyses des supports est également recherchée. Cette interaction n'est pas possible avec un expert civil qui est commis ou réquisitionné et qui mène principalement ses opérations en autonomie et donc de manière isolée.

340. Cette puissance d'investigation par des services spécialisés est renforcée par le fait que les autorités judiciaires peuvent, notamment en matière de cryptologie[495] ou de captation de données[496], saisir les moyens de l'Etat[497], ce que ne peuvent évidemment pas faire les experts.

341. Le passage par la liste des experts pour contourner la limitation dans l'exploitation des scellés. – Se pose alors naturellement la question de savoir comment, sans violer les règles de procédure, les enquêteurs parviennent à saisir ces services spécialisés pour analyser les supports numériques saisis au cours d'une perquisition, postérieurement à leur inventaire[498].

---

[492] V. *infra* n°342.

[493] Ces services disposent d'infrastructures matérielles avec d'importantes capacités pour, notamment, procéder à des attaques par force brute (c'est-à-dire essayer toutes les combinaisons possibles de caractères) sur des mots de passe. Ils sont également équipés de suite logicielles forensiques beaucoup plus étoffées que l'équipement fourni aux N'Tech ou aux ESCI.

[494] En cryptologie, en logiciel de cryptage, en failles de sécurité naturellement présentes dans les logiciels ou systèmes d'exploitation.

[495] C. pr. pén. art. 230-2 : « Lorsque le procureur de la République, la juridiction d'instruction […] ou la juridiction de jugement saisie de l'affaire décident d'avoir recours […] aux moyens de l'Etat couverts par le secret de la défense nationale […]. » - V. *infra* n°408.

[496] C. pr. pén. art. 706-102-1 – Pour une étude détaillée de la mesure, v. *infra* n° 570.

[497] C'est-à-dire les moyens dont disposent les services de renseignement : v. *ibid.* sur les moyens matériels.

[498] V. *supra* n°328.

342. Un retour sur les listes des experts judiciaires, précédemment décrites[499] est nécessaire. Les forces de police et de gendarmerie ont deux moyens pour intervenir dans le cadre d'une expertise en bonne et due forme[500]. Tout d'abord, certains laboratoires internes à la police judiciaire sont inscrits sur l'une des listes des experts judiciaires en tant que personne morale[501]. Cette situation est toutefois peu courante.

343. Ensuite, beaucoup plus fréquemment, ce sont les agents de ces laboratoires qui sont inscrits sur une liste d'experts judiciaires en tant que personne physique[502]. Cela permet donc à des enquêteurs de terrain de pouvoir réquisitionner, ou à des juges d'instructions de commettre, des experts qui sont en fait des militaires de la Gendarmerie ou des agents de la Police nationale.

344. Un détournement de la liste des experts judiciaires. – Ces deux méthodes pour faire appel à des techniciens compétents en numérique internes à la Gendarmerie ou la Police nationales, constituent un détournement de la liste des experts judiciaires. En effet, la raison d'être des experts, est de pouvoir faire appel à des compétences techniques de personnes issues de la société civile. Il y a clairement un objectif de dissocier le pouvoir d'enquête des investigations diligentées sur des supports numériques. Or, dans ces deux cas de figure, les experts ne sont pas indépendants puisqu'ils font partie d'une chaîne de commandement ou hiérarchique qui les lie inextricablement aux enquêteurs qui œuvrent dans le dossier. Le principe d'impartialité qui fait partie des règles qui s'imposent aux experts n'est, en aucun cas, respecté[503].

345. De plus, le cas des militaires ou des agents qui sont inscrits en leur nom propre soulève d'autres questions. Outre les personnes morales inscrites sur les listes d'experts et qui sont marginales en termes de quantité, le principe de l'expertise est de commettre des personnes physiques qui, par là-même, engage leur responsabilité individuelle[504]. Ce

---

[499] V. *supra* n°301.

[500] Ou dans le cadre d'une réquisition à expert : v. *supra* n°305.

[501] Exemple : Institut National de Police Scientifique – 31, avenue Franklin Roosevelt 69134 ECULLY CEDEX qui est inscrit sur la liste des experts près la Cour d'Appel de Lyon.

[502] Exemples : agents du laboratoire de police scientifique de Toulouse sur la liste des experts près la Cour d'appel de Toulouse, militaires de l'Institut de Recherche Criminelle de la Gendarmerie Nationale sur la liste des experts près la Cour d'appel de Paris, etc.

[503] BOULEZ Jacques, *Expertises judiciaires – Désignation et mission de l'expert – Procédure selon la juridiction*, 13ème édition, DELMAS, p. 57 et 58.

[504] LARRIBEAU-TERNEYRE Virginie, *La responsabilité de l'expert judiciaire; à l'ombre du droit commun de la responsabilité civile,* Les Petites Affiches, 2 déc. 1998, p.7 : « la responsabilité de l'expert à raison d'un préjudice qui serait lié à l'exercice de sa mission est une responsabilité civile ordinaire, fondée sur l'article 1382 du Code civil : cette responsabilité, qui aboutit à une condamnation personnelle de l'expert au paiement de dommages-intérêts, est la responsabilité de droit commun par excellence. »

mécanisme devient particulièrement obscur dans le cas d'un agent ou d'un militaire qui, bien évidemment, procède aux investigations dans le cadre de ses fonctions, mais qui est désigné nominativement par une juridiction d'instruction.

β. Un contournement pour gagner en vitesse et fluidité

346. Les longs délais de l'expertise informatique. – Les experts judiciaires en informatique sont principalement saisis au stade de l'information judiciaire. En effet, les délais qui se pratiquent usuellement pour une telle mission sont compris entre deux et quatre mois. Le cadre processuel qui entoure l'instruction est compatible avec cela. En revanche, en enquête de flagrance, les experts en informatique ne sont jamais requis pour analyser un support numérique. Leur intervention est incompatible avec les contraintes temporelles inhérentes à cette procédure[505]. Avec la baisse d'ouverture d'informations judiciaires[506], l'enquête préliminaire prend de plus en plus d'importance. Par voie de conséquence, le besoin d'analyser des supports contenant des données augmente. Pour autant, la réquisition d'expert existe à ce stade mais elle n'est pas fréquente, essentiellement en raison d'un besoin de rapidité qui reste important et incompatible avec les délais usuellement nécessaires aux expertises informatiques.

347. L'analyse des scellés saisis en perquisition par les enquêteurs. – Les règles pour analyser des objets contenant des données sont moins strictes en enquête qu'en information judiciaire[507]. Pour autant, les enquêteurs sont rigoureux et vigilants pour que ces scellés ne soient pas analysés par les mêmes personnes qui participent à l'enquête[508].

348. Une première solution apportée par la loi du 3 juin 2016. – La loi du 3 juin 2016[509] a créé l'article 60-3 dans le Code de procédure pénale[510], dont la finalité paraît directement destinée à contourner la limitation imposée pour l'exploitation des scellés

[505] C. pr. pén. art. 53 et s.
[506] En 2016, seulement « 5% des affaires pénales poursuivables » faisaient l'objet d'une information judiciaire contre 41% en 1835. Source : Ecole Nationale de la Magistrature de Bordeaux.
[507] V. *supra* n°325.
[508] Dans la Gendarmerie, par exemple, les N'Tech sont le plus souvent également officier de police judiciaire et peuvent donc cumuler les deux fonctions. V. *infra* n°350.
[509] *Op. cit.* p.23 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.
PERRIER Jean-Baptiste, *Les garanties de la procédure pénale dans la loi du 3 juin 2016 : entre illusion(s) et désillusion(s),* Recueil Dalloz 2016 p.2134.
[510] Transposé en enquête préliminaire avec l'article 77-1-3 et à l'instruction avec le 99-5.

saisis en perquisition[511]. Celui-ci utilise le fait que les experts peuvent briser les scellés et exploiter leur contenu en dehors de la présence des personnes ciblées par la perquisition, contrairement aux enquêteurs[512]. En effet, cet article prévoit que des experts soient requis uniquement pour cloner le support de données informatiques objet du scellé, c'est-à-dire sans procéder à la moindre exploitation de son contenu. Cette disposition est la consécration légale du don d'ubiquité des données numériques[513].

349. Le clonage de ces données est réalisé « afin de permettre leur exploitation sans porter atteinte à leur intégrité ». Or, de quelle exploitation s'agit-il ? Pourquoi le législateur a-t-il pris la peine d'introduire cet article si ce n'est pour permettre aux enquêteurs ou à leurs services spécialisés d'exploiter les données contenues dans ces scellés d'une manière différente de celles prévues ? Il est aisé de comprendre que l'idée est ici de jouer sur le don d'ubiquité d'un support numérique, en faisant procéder au clonage des données selon une procédure stable (c'est-à-dire par un expert), puis d'en faire analyser le contenu par des policiers ou des gendarmes. Si, ultérieurement, la personne à qui sont opposées les éventuelles preuves extraites de ces investigations les conteste, les autorités judiciaires pourraient saisir un expert[514] selon la procédure « standard[515] ».

350. Les enquêteurs[516] confirment qu'ils se sont emparés de cette nouvelle possibilité et l'utilisent abondamment, surtout au stade de l'enquête de flagrance ou préliminaire. Au sein de la gendarmerie, l'usage veut que les enquêteurs réquisitionnent un N'Tech en qualité de sachant (bien que non inscrit sur une liste d'experts) pour procéder au clonage, en prenant toutefois la précaution que celui-ci n'ait pas des fonctions de police judiciaire au sein de ce dossier[517]. Il ne reste plus alors qu'à confier l'analyse de l'image ainsi obtenue à un autre N'Tech différent de celui qui a cloné.

---

[511] V. *supra* n°325.
[512] V. *supra* n°304.
[513] V. *supra* n°227.
[514] Cette expertise serait, dans les faits, une contre-expertise. Sur le régime de la demande d'une contre-pertise, v. Crim. 4 dec. 2007 n°07-87.047 : JurisData n°2007-042022. BUISSON Jacques, Les ordonnances refusant un complément d'expertise ou une contre-expertise ne subissent plus le filtrage du président, LexisNexis Procédures n° 2, Février 2008, comm. 57.
[515] V. *supra* n°304.
[516] TONELLI Stéphane, Chef du groupe cybercriminalité, Section de Recherche de Toulouse, Gendarmerie Nationale, entretien du 1er décembre 2017.
[517] L'objectif est d'éviter qu'une même personne cumule des fonctions « d'expert » et d'officier de police judiciaire.

351. Une deuxième étape franchie avec la loi du 23 mars 2019[518]. – Cette dernière introduit une nouvelle étape dans la prise en compte par les pouvoirs publics, des difficultés de l'intervention des experts judiciaires au sein des investigations numériques. Le nouvel article 157-2 dispose que « l'expertise peut également être demandée à des services ou organismes de police technique et scientifique de la police nationale et de la gendarmerie nationale dont la liste est fixée par arrêté conjoint du ministre de la justice et du ministre de l'intérieur ». Cette disposition est d'une portée générale pour l'ensemble des expertises et dépasse donc le cadre des investigations numériques, contrairement au nouvel article 60-3 qui leur était entièrement consacré. Néanmoins, le contournement des listes d'experts judiciaires qui en ressort fait écho aux situations qui viennent d'être évoquées sur ce point. La création de cet article, passée inaperçue dans la doctrine, appelle plusieurs commentaires.

352. En premier lieu, l'introduction d'une liste parallèle aux listes d'experts judiciaires[519] soulèvent une difficulté pratique. Que deviennent les enquêteurs spécialisés ou les laboratoires de police scientifique qui sont inscrits sur les listes actuelles[520] ? Quoi qu'il en soit, c'est une source d'instabilité qui est introduite ici dans le travail quotidien du juge qui va devoir choisir entre deux listes, au sein desquelles certaines personnes seront inscrites en double.

353. En second lieu, la loi de mars 2019 a créé une instabilité dans la procédure pénale au travers de cette nouvelle disposition, car l'article 157 qui évoque les listes d'experts judiciaires est cité par de nombreux autres articles du Code[521]. A aucun moment ces autres articles n'ont été modifié en incluant une référence à cette nouvelle liste prévue à l'article 157-2. Encore une fois, une source d'instabilité apparaît pour le juge qui peut être tenté de choisir quelqu'un de la liste parallèle pour une investigation définie par un article qui se limite à viser les listes de l'article 157.

354. Des mesures de contournement contestables. – Il paraît regrettable que le législateur ait choisi de mettre en place ces mesures de contournement, procédant par petites touches, plutôt que de réformer en profondeur ce point de la procédure pénale

[518] Loi n°2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice. *Op. cit.* p.18.
[519] V. *supra* n°301.
[520] V. *supra* n°342.
[521] V. par ex. C. pr.pén. art. 60 pour la réquisition (v. *supra* n°305.) ou l'art.706-102-1 pour la captation des données (v. *infra* n°570.)

relatif aux analyses des supports numériques. La nécessité d'offrir la possibilité au magistrat de les confier directement à des services spécialisés de la Police ou de la Gendarmerie semble indispensable. En effet, tout d'abord, la façon de procéder qui consiste à cloner un support pour confier l'analyse de la copie à un enquêteur laisse planer un doute important sur la stabilité d'une telle procédure : si la nullité de l'analyse de la copie des données venait à être soulevée[522] au motif que les investigations ont été réalisées en dehors de la présence de la personne poursuivie, comment pourrait-on justifier qu'une expertise soit ordonnée précisément sur le support au sein duquel ont été retrouvées des preuves précédemment annulées ?

355. Ensuite, quand bien même l'annulation serait écartée, la perte de temps dans l'enquête serait importante. Cette perte de temps est d'ailleurs présente dès l'origine de cette façon de procéder, puisque le seul fait de devoir saisir un expert pour procéder à un clonage des supports mis sous scellés, peut s'avérer importante dans des dossiers où chaque instant compte.

356. Conclusion du sous-paragraphe A : la fouille des scellés numériques. – La procédure pénale génère une grande confusion dans l'analyse de scellés contenant des informations numériques. La saisie d'un expert, pourtant instaurée comme la voie usuelle, nuit généralement à l'efficacité de l'enquête, notamment en allongeant énormément les délais[523]. D'ailleurs, les autorités publiques ont pris conscience de cette situation puisqu'en juin 2016, et en mars 2019, deux nouvelles dispositions ont été introduites afin d'offrir aux enquêteurs la possibilité de conserver, sous leur contrôle, les analyses des données présentes dans un scellé. Dans ces conditions, quand et pourquoi faire appel à un expert judiciaire ou aux enquêteurs spécialisés de la police ou de la gendarmerie pour procéder à des analyses sur ce type de scellés ? La présente étude propose une clarification de cette situation[524], grâce à l'optimisation de l'exploitation des données[525], point commun de toutes les investigations numériques.

357. Les actes de procédures autorisant explicitement la fouille des données sont peu nombreux. Outre la fouille des scellés contenant des informations numériques, les autorités judiciaires peuvent investiguer dans les messageries dématérialisées.

---

[522] Sur le régime des nullités, v. *infra* n°856.
[523] V. *infra* n°931.
[524] V. *infra* n°936.
[525] V. *infra* n°799.

B. La fouille des messageries numériques

358. L'accès, l'extraction et l'enregistrement de données. – Les articles 706-95-1 et suivants du Code de procédure pénale créent une investigation numérique dont l'objet est de fouiller le contenu des messages numériques échangés et, le cas échéant, d'en extraire des données et de les enregistrer[526].

Les conditions de mise en œuvre *(1)* et les effets *(2)* de cet acte sont distingués pour plus de lisibilité.

1. La mise en œuvre de la fouille des messageries numériques

359. Une mise en œuvre dépassant la criminalité organisée. – La fouille des messageries numériques est prévue au sein de la procédure spéciale réservée à la criminalité et à la délinquance organisées, et est étendue aux infractions en matière sanitaire et environnementale[527]. La loi du 23 mars 2019[528] a considérablement élargi les conditions de mise en œuvre de cette investigation numérique, en la généralisant à tous les crimes. Cette extension doit être soulignée car le Conseil constitutionnel a censuré[529] la même intention pour d'autres investigations numériques[530], au motif que ces dernières sont « particulièrement intrusives pour des infractions ne présentant pas nécessairement un caractère hautement complexe, sans assortir ce recours des garanties permettant un contrôle suffisant par le juge du maintien du caractère nécessaire et proportionné de ces mesures durant leur déroulé ».

360. Une distinction infondée. – Le Conseil a retenu le critère de mesures « particulièrement intrusives » pour refuser l'extension aux crimes, d'investigations numériques comme, par exemple, la sonorisation et la fixation d'images. Il en résulte une distinction incompréhensible entre la fouille des messageries numériques et ces autres

[526] C. pr. pén. art 706-95-1 : « […] Les données auxquelles il a été permis d'accéder peuvent être saisies et enregistrées ou copiées sur tout support. »
C. pr. pén. art 706-95-1 *idem.*
[527] C. pr. pén. art. 706-2-2
[528] Loi n°2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice (*op. cit.* p.18)
[529] Conseil constitutionnel, décision n°2019-778 DC du 21 mars 2019.
MAYAUD Yves, *De la loi au Conseil constitutionnel, une réforme contrastée de la procédure pénale*, Dalloz, AJ pénal 2019, p. 176 : « […] à se reporter aux censures du Conseil constitutionnel, l'habileté est souvent défaillante, d'où un contraste non négligeable entre ce que le législateur souhaitait et ce qui lui est finalement concédé […]. »
[530] Dispositions censurées au sein de l'article 706-95-11 qui auraient étendu aux crimes trois investigations numériques présentes dans les techniques spéciales d'enquête.

investigations numériques. En quoi la sonorisation et la fixation d'images seraient plus intrusives que la fouille des messageries numériques ? En effet, cette dernière est hautement attentatoire à la vie privée, tant les correspondances dématérialisées sont un support essentiel à la vie personnelle et professionnelle de tout individu.

361. La démarche d'homogénéisation des actes d'enquête par la loi du 23 mars 2019 inachevée. – La loi de mars 2019 avait pour ambition d'homogénéiser les actes d'enquête[531]. Ce fut notamment le cas avec les mesures de surveillance[532] pour lesquelles le législateur a créé un paragraphe « dispositions communes » en ce sens, qui évite une redondance systématique des articles[533]. Or, dans le cas de la fouille des messageries, cette homogénéisation n'a pas été appliquée puisque, de manière assez regrettable, il perdure une décomposition des dispositions en deux articles. Ainsi, un article concerne la mise en œuvre au stade de l'enquête[534] et un autre l'information judiciaire[535].

2. Les effets de la fouille des messageries numériques

362. De nombreuses cibles. – Les articles 706-95-1 et suivants du Code de procédure pénale ciblent toutes les « correspondances stockées par la voie des communications électroniques accessibles au moyen d'un identifiant informatique », ce qui ouvre un vaste champ d'application.

363. Les messageries électroniques. – En premier lieu, ces dispositions concernent les messageries dématérialisées. Grâce à une évolution des techniques et des usages, cette investigation numérique est d'une redoutable efficacité. En effet, jusqu'au début des années 2000, les utilisateurs géraient leurs courriers électroniques avec des clients de messagerie[536], et selon un protocole[537] qui relevaient les messages et les stockaient sur le disque dur local de l'ordinateur utilisé. Le fonctionnement était identique à une boîte à lettres physique : cette dernière est vidée chaque fois que l'on va chercher le courrier.

[531] V. *supra* n°238.
[532] V. *infra* n°441.
[533] Un article destiné à l'enquête et un autre pour l'information judiciaire.
[534] C. pr. pén. art. 706-95-1.
[535] C. pr. pén. art. 706-95-2.
[536] Comme Microsoft Outlook, Thunderbird, etc.
[537] *Pop 3*.

364. Désormais, l'usage le plus courant est de laisser les messages sur le serveur. C'est le cas avec les messageries gérées en mode *webmail*[538], mais également avec les clients de messagerie qui utilisent des protocoles[539] qui font que les messages restent sur le serveur. Le logiciel local synchronise les messages entre ce serveur et les mails affichés par l'ordinateur. Dans ce contexte, les dispositions des articles 706-95-1 et suivants sont très efficaces en autorisant les enquêteurs à accéder directement au serveur de messagerie. C'est ainsi un accès complet à la correspondance dématérialisée d'une personne qui est offert[540].

365. Les autres outils d'échanges. – En second lieu, la formulation du texte est telle que la cible de cette investigation numérique dépasse les messageries électroniques. En effet, ce sont tous les systèmes permettant d'échanger des correspondances qui sont visés. Les réseaux sociaux[541] et les messageries instantanées[542] entrent dans cette catégorie.

366. Un acte très proche de la perquisition dans ses effets. – Les messageries sont des espaces numériques privés. Ils sont « privés » parce qu'accessibles avec un *login* nominatif (le texte parle « d'identifiant informatique[543] »). Il est alors nécessaire de s'interroger si la fouille des messageries n'est pas une véritable perquisition de celles-ci. Aucune réponse catégorique à cette question ne se dégage de la doctrine. Certains auteurs pensent que le critère de « pénétration d'un lieu normalement clos[544] », présent dans la définition de la perquisition[545], n'est pas vérifié avec une fouille de données à distance[546]. Néanmoins, cette affirmation est nuancée avec d'autres auteurs qui n'hésitent pas à parler

[538] Exemples : *Gmail*, *Hotmail,* des solutions internes aux entreprises (v. GENGEMBRE Charles, *Information sensible d'entreprise : une attention de tous les instants*, ItforBusiness, 14 mars 2018 : « […] la consommation de nouveaux outils de stockage s'est largement démocratisée, multipliant d'autant les localisations et copies de la donnée […]. »)
[539] *Imap*.
[540] Messages reçus, envoyés, brouillons enregistrés.
[541] Les réseaux sociaux proposent tous des systèmes de messagerie interne. Ex. : Facebook avec Messenger, Instagram, etc.
[542] Ex. : *Whatsapp*, *Hangout*, etc
[543] C. pr. pén. art. 706-95-1, 406-95-2 et 706-95-3
[544] Sur la notion de lieu clos, v. DESPORTES Frédéric et LAZERGES-COUSQUER Laurence, *Traité de procédure pénale,* Economica, p.1407 et s.
V. eg. PRADEL Jean, *Définition de la perquisition : notion de lieu clos,* Recueil Dalloz 1995 p.144 : « […] La perquisition suppose une pénétration dans un lieu. […] »
[545] V. *supra* n°244.
[546] DECIMA Olivier, *Du piratage informatique aux perquisitions et saisies numériques ?* Dalloz AJ pénal 2017 p.315.

de « domicile virtuel[547] » dans le cas d'espace numérique privé. En revanche, la doctrine est unanime pour relever le caractère particulièrement attentatoire aux libertés individuelles d'une mesure dont les effets sont très proches de la perquisition. Cette dernière, en raison de son cadre très strict, offre des garanties qui sont totalement absentes de la fouille des messageries.

367. Une durée non limitée. – Tout d'abord, la perquisition est limitée dans le temps, contrairement à la fouille des messageries pour laquelle les dispositions n'apportent aucune précision quant à la durée ou au nombre de réitérations. Ainsi, rien n'empêche les enquêteurs de fouiller la boîte mails d'un individu quotidiennement pendant plusieurs mois.

368. Une absence totale d'information. – Ensuite, le respect de la vie privée est d'autant plus mis à mal au travers de la fouille des messageries que, contrairement à la perquisition qui est nécessairement portée à la connaissance du propriétaire des lieux[548], cette investigation numérique ne laisse aucune trace et rien n'oblige les autorités judiciaires à informer la personne visée par la mesure. De plus, la loi du 23 mars 2019[549] a introduit, sous certaines conditions, la possibilité pour la personne perquisitionnée de demander l'annulation de l'acte si aucune poursuite n'est engagée dans un délai de six mois[550]. A aucun moment, une telle possibilité n'est offerte en cas de fouille de messageries numériques.

369. Une limitation neutralisée. – Les précautions selon lesquelles « les opérations […] ne peuvent, à peine de nullité, avoir un autre objet que la recherche et la constatation des infractions visées dans la décision […][551] » sont peu protectrices, puisque, dans le même temps, « le fait que ces opérations révèlent des infractions autres que celles visées dans la décision du magistrat qui les a autorisées ne constitue pas une cause de nullité des procédures incidentes[552] ». La seule protection qu'offrent réellement ces dispositions,

---

[547] SAINT-PAU Jean-Christophe, *Les investigations numériques et le droit au respect de la vie privée,* Dalloz AJ pénal 2017, p.321.
DUMENIL Gabriel, *Vers une dématérialisation du domicile : réflexions autour de la théorie du domicile virtuel en droit pénal,* LexisNexis, Droit pénal n° 7-8, Juillet 2019, étude n°17.
[548] Si le propriétaire des lieux n'est pas présent, des témoins doivent assister à la perquisition.
[549] *Op. cit.*
[550] V. *supra* n°287.
[551] C. pr. pén. art 706-95-3.
[552] *Ibid.*

couvre le cas d'un détournement de procédure, c'est-à-dire le cas où des enquêteurs se placeraient « faussement et à dessein dans le champ d'application[553] » des procédures dérogatoires au sein desquelles la fouille des messageries est autorisée[554]. Or, ce moyen de nullité est rarement retenu par la Cour de cassation[555].

370. Conclusion du sous-paragraphe I. – Quantitativement, la procédure pénale comporte peu d'actes autorisant explicitement la fouille de données en dehors du cadre de la perquisition. Historiquement, la démarche s'est construite sur une chronologie des actes : des objets sont saisis lors d'une perquisition et sont exploités dans un second temps. C'est dans cette logique que l'exploitation des supports numériques, soit par l'intermédiaire des experts, soit par les enquêteurs eux-mêmes, intervient. Mais la numérisation de notre société fait naître de nouveaux besoins, avec la nécessité pour les autorités judiciaires de pouvoir fouiller des espaces numériques particuliers, comme les messageries dématérialisées. Ces besoins ont donné naissance à des actes particulièrement ambigüs, car très proches de la perquisition dans leurs effets, mais sans offrir les garanties de cette dernière, notamment en termes de limitation dans le temps et d'information de la personne visée par la mesure.
Cette ambiguïté s'accentue encore avec une autre catégorie d'actes qui ne comporte pas la notion de fouille des données et qui, pourtant, l'autorise implicitement.

II – <u>Des fouilles implicites</u>

371. La fouille découlant de l'objectif de l'acte. – Certaines investigations numériques ne font pas explicitement références à la fouille des données. Pourtant, cette fouille découle de l'objectif de la mesure. C'est le cas avec les réquisitions adressées à des tiers à la procédure *(A)* ainsi qu'avec le déchiffrement des données *(B)*.

[553] Crim. 18 juin 2019 n°19-80.015 : JurisData n°2019-010591 – FOURMENT François, *Détournement de procédure, fraude au champ d'application d'un pouvoir d'enquête ou d'instruction,* LexisNexis, Droit pénal n°9, Septembre 2019, comm. 156.
[554] V. *supra* n°359.
[555] *Ibid.* FOURMENT François : la notion de détournement de procédure n'apparaît que dans 9 arrêts depuis 1963.

A. L'obtention de données auprès de tiers

372. La notion de « tiers à la procédure ». – L'adaptation de la procédure pénale à la numérisation de notre société au travers de la dématérialisation des investigations[556] se matérialise parfaitement avec la prise en considération que des éléments numériques peuvent être détenus par un tiers étranger aux faits criminels ou délictuels à l'origine de l'ouverture d'une procédure, et pourtant susceptibles d'intéresser les faits. En fait, ce tiers se trouve impliqué comme une sorte de témoin par détention d'éléments numériques. C'est ce que certains auteurs appellent « l'accès indirect » à des documents ou des informations numériques[557].

373. L'obtention de données. – Les actes permettant d'obtenir ces informations auprès d'un tiers prévoient qu'elles le soient sous la forme de données[558], ce qui est une condition indispensable pour caractériser une investigation numérique[559].

374. Une investigation numérique intrusive. – L'obtention d'informations numériques auprès de tiers est tout aussi intrusive que d'autres actes de fouille de données. En effet, les enquêteurs s'intéressent ici à l'environnement numérique d'un individu ciblé par l'enquête, ce qui peut les conduire à obtenir des informations personnelles et privées[560].

Pour obtenir ces données, un certain flou entoure, aussi bien la mise en œuvre des actes correspondants *(1)*, que leurs effets *(2)*.

1. La mise en œuvre de l'obtention des données auprès de tiers

375. Deux actes de procédure pour réquisitionner des données. – L'obtention de données auprès de tiers étrangers aux faits à l'origine de l'ouverture d'une enquête, utilise le principe de la réquisition *(a)*. Malheureusement, deux actes cohabitent dans le Code de procédure pénale pour procéder à celle-ci *(b)*, ce qui génère un flou important.

---

[556] V. *supra* n°53.

[557] *Op. cit.* p.35, MICHALSKI Cédric, *La recherche et la saisie des preuves électroniques*, Gazette du Palais 11 fév. 2014 n°42.

[558] C. pr. pén. art. 60-1 : « […] de lui remettre ces informations, notamment sous forme numérique […]. » C. pr. pén. art. D15-5 : « Lorsque les documents requis sont transmis sous forme numérique, le cas échéant par un moyen de communication électronique, ils sont annexés sous format papier ou numérique au procès-verbal. »

[559] V. *supra* n°206.

[560] Identification des titulaires d'une ligne téléphonique (Crim. 27 mars 2018 n°17-85.603 : JurisData n°2018-004696), historique de la localisation d'un téléphone (Crim. 2 nov. 2016 n°16-82.376 : JurisData n°2016-022725), vidéosurveillance mise en œuvre par une entreprise privée (Crim. 9 fév. 2016 n°15-85.069 : Jurisdata n°2016-001953), etc.

a. L'obtention des données par les réquisitions

376. La réquisition pour obtenir des informations. – Pour obtenir des informations auprès de tiers, les autorités judiciaires utilisent une réquisition[561]. Les actes correspondants font partie de la procédure de droit commun, puisqu'ils peuvent être mis en œuvre pour toute infraction punie d'une peine d'emprisonnement. Tout comme la perquisition, dont l'objet dépasse nettement la recherche de données, la réquisition permet d'obtenir, auprès de tiers, toute sorte d'informations[562].

377. Une pluralité de réquisitions en procédure pénale. – Le mot « réquisition » est fréquemment utilisé en procédure pénale[563] et il est donc nécessaire de définir précisément la différence avec les autres réquisitions qui existent.

378. Deux autres types de réquisitions. – En premier lieu, les officiers de police judiciaire peuvent s'adjoindre les compétences d'un « sachant » en le réquisitionnant afin, notamment, de procéder à des analyses de supports numériques[564]. En second lieu, des réquisitions spécifiques peuvent être délivrées à l'égard de tiers techniques, pour installer des dispositifs lors des interceptions de correspondances ou de la captation de données[565].

379. Une distinction par la prestation de serment. – Les réquisitions qui permettent d'obtenir des données, des documents ou des informations numériques auprès de tiers, se rapprochent de celles permettant d'installer des dispositifs en ceci que la personne réquisitionnée intervient en qualité « d'opérateur ». En effet, dans ces deux cas, aucune action d'interprétation ou d'analyse, n'est demandée à la personne réquisitionnée. Ainsi, fort logiquement, il n'est pas imposé aux personnes réquisitionnées dans ce cas de figure, de prêter serment[566]. *A contrario*, les personnes saisies au titre de l'article 60, pour leur

[561] C. pr. pén. art. 60-1, 77-1-1 et 99-3, respectivement en enquête de flagrance, préliminaire et au cours de l'information judiciaire.
[562] Par ex. des documents papiers remis par un individu faisant l'objet d'une enquête, à une banque ou un assureur.
[563] Pour une définition de la réquisition, v. MATHONNET Paul et GHNASSIA Michaël, *La Cour de cassation pose ses conditions en matière de réquisitions de documents délivrées au cours des enquêtes préliminaires* — Recueil Dalloz 2006 p.1429 : « Par réquisition, il faut entendre une demande écrite ou verbale délivrée par l'autorité publique, administrative ou judiciaire à une personne physique ou morale, de droit privé comme de droit public, d'accomplir un acte ou une prestation. »
[564] C. pr. pén. art. 60 et 77-1. V. *supra* n°305.
[565] Pour les écoutes téléphoniques : C. pr. pén. art. 100-3 : « ou tout agent qualifié d'un exploitant de réseau ou fournisseur de services de télécom. » - Pour la captation des données, v. *infra* n°583.
[566] Crim. 18 juin 2002 n°01-86.098 ; Bull. crim. n°136 : « L'identification de numéros de téléphone auprès d'un opérateur n'est pas une mesure de constatation ou d'examen technique ou scientifique au sens des articles 60 et 77-1 du Code de procédure pénale. Le directeur régional de l'opérateur téléphonique en

part, procèdent à des investigations, notamment sur des données s'il s'agit d'un support numérique à analyser. En conséquence, elles participent activement à la recherche de preuves.

380. Le critère de l'absence de prestation de serment lors de la mise en œuvre des dispositions permet de classer la réquisition d'informations auprès de tiers au sein des différentes réquisitions qui existent en procédure pénale.

Néanmoins, une ambiguïté supplémentaire réside dans le fait que deux séries d'actes sont prévues pour parvenir à cette obtention de données.

b. Deux actes pour les réquisitions des données

381. Le chevauchement de deux groupes de dispositions. – L'article 60-1 n'est pas la seule disposition permettant de réquisitionner des informations auprès d'un tiers. Il existe un deuxième groupe de dispositions[567], qui permet d'obtenir un résultat similaire.

382. L'étrange maintien de dispositions plus anciennes. – Le maintien dans le Code de procédure pénale de l'article 60-2 après la création de l'article 60-1 pousse à s'interroger sur la pertinence de la cohabitation de ces deux séries de dispositions. En effet, ces articles 60-2 et 77-1-2 datent de la loi n°2003-239 du 18 mars 2003 pour la sécurité intérieure. Ils étaient précédemment codifiés sous les numéros 60-1 et 77-1-1 jusqu'à la loi n°2004-204 du 9 mars 2004 portant adaptation de la justice aux évolutions de la criminalité, qui les a renumérotés sous leur forme actuelle, en créant les articles 60-1 et 77-1-1. Le doute quant à la pertinence du maintien de ces dispositions se confirme au travers de la jurisprudence puisque l'article 60-2 est peu présent dans les décisions de la Cour de cassation[568]. Cette inutilisation trouve certainement sa source dans le premier alinéa de l'article 60-2 qui vient chevaucher les dispositions de l'article 60-1. La Cour de cassation ne vise donc ces anciennes dispositions que de manière marginale, pour justifier des réquisitions d'opérateurs téléphoniques pour obtenir la « communication de données

question n'est donc pas tenu de prêter serment. » ROTH Cyril – LEPRIEUR Anne – DIVIALLE Marie-Luce, *Chronique de jurisprudence de la Cour de cassation*, D. 2012, p.171.

[567] C. pr. pén. art. 60-2, 77-1-2 et 99-4 respectivement en enquête de flagrance, préliminaire et au cours de l'information judiciaire.

[568] Crim. 9 nov. 2011 n°11-84.315 JurisData n°2011-028835: les motifs pour invoquer l'annulation d'un arrêt d'une chambre d'instruction visent à la fois les articles 77-1-1 et 77-1-2 du Code de procédure pénale. La Cour, pour justifier son rejet, ne s'intéresse qu'à l'article 77-1-1 ; Crim. 6 dec. 2005 n°05-85.076 Bull. crim. n°319 et Crim. 6 février 2018 n°17-84380 B. n°48: *idem*.

de téléphonie[569] ». Ce sont donc les articles 60-1 et 77-1-1 qui sont quasiment systématiquement utilisés lors de réquisitions auprès des opérateurs de téléphonie aux fins d'obtenir les informations de la ligne et de son activité.

383. Les ambiguïtés issues du chevauchement entre ces deux dispositions se prolongent dans les effets des réquisitions de tiers pour obtenir des données.

2. Les effets de l'obtention de données auprès de tiers

384. Un effet coercitif très limité. – Lorsque les autorités judiciaires réquisitionnent un tiers pour obtenir des informations en application des articles 60-1 ou 60-2 du Code de procédure pénale, le fait de s'abstenir ou de refuser de répondre est puni d'une amende de 3 750 euros[570]. Outre le montant dérisoire de la sanction, tout particulièrement pour une entreprise de taille importante, la formulation des dispositions donne l'impression qu'il s'agit d'une simple demande[571] formulée au tiers, avec un aspect peu coercitif.

385. De plus, l'efficacité de cette demande est limitée, car les actes correspondants ne permettent pas d'obtenir toutes les données qui pourraient être utiles *(a)*. En revanche, alors que l'objectif de ces investigations numériques et de se faire remettre des informations numériques enregistrées chez un tiers, la fouille des données ainsi recueillies n'est explicitement autorisée par le texte *(b)*.

a. La limitation du périmètre des données

386. Les réquisitions formulées auprès d'un tiers peuvent laisser croire, à la lecture du texte, que l'on peut obtenir une très large catégorie de données *(a)*.

Or, ce n'est pas le cas, car les deux séries de dispositions permettant de solliciter ce tiers, ne s'imbriquent pas efficacement pour autoriser l'obtention d'un large éventail d'informations numériques *(b)*.

---

[569] Crim. 21 juin 2011 n°11-81.846 : JurisData n°2011-014804. *Obs.* QUEMENER Myriam, *Les spécificités juridiques de la preuve numérique,* Dalloz AJ Pénal 2014 p.63 (*op. cit.* p.35).

[570] C. pr. pén. art. 60-1 : « A l'exception des personnes mentionnées aux articles 56-1 à 56-5, le fait de s'abstenir de répondre à cette réquisition dans les meilleurs délais et s'il y a lieu selon les normes exigées est puni d'une amende de 3 750 euros. »
C. pr. pén. art. 60-2 : « Le fait de refuser de répondre sans motif légitime à ces réquisitions est puni d'une amende de 3 750 euros. »

[571] L'article 60-2 parle de « mettre à disposition des informations ».

α. Un large éventail de données en apparence

387. Deux catégories de données. – Lors de la mise en œuvre de l'obtention d'informations numériques auprès d'un tiers, les enquêteurs peuvent obtenir deux typologies distinctes de données. Ces dernières ressortent de la formulation de l'article 60-1, qui parle « des informations intéressant l'enquête, y compris celles issues d'un système informatique ou d'un traitement de données nominatives […] ». La première catégorie est aisément cernable tandis que la deuxième semble, à tort, beaucoup plus vaste.

388. Une première catégorie au périmètre clair. – Les informations provenant d'un « traitement de données nominatives » sont faciles à délimiter puisqu'il s'agit, par exemple, de l'historique des connexions à Internet détenu par les fournisseurs d'accès ou encore l'activité d'une ligne téléphonique[572]. Ces informations sont précieuses pour l'enquête car les fournisseurs d'accès à Internet sont les seuls capables de pouvoir indiquer à quel abonné est attribuée une adresse IP publique[573] ou un numéro d'une ligne mobile.

389. Une deuxième catégorie difficile à circonscrire. – Lorsque l'article 60-1 prévoit que des informations « issues d'un système informatique » peuvent également être demandées, un périmètre beaucoup plus flou est alors ouvert. En effet, la notion de système informatique peut être entendue très largement[574], puisqu'il est possible de considérer que tout fichier[575] détenu par « un établissement ou un organisme public ou privé », ou encore par « une administration publique », entre dans le champ de cette disposition à la seule condition qu'il intéresse l'enquête. C'est à ce titre que les autorités judiciaires peuvent demander des vidéos extraites d'un dispositif de vidéoprotection[576] à

[572] *Op. cit.* p. 35 Crim. 21 juin 2011 n°11-81.846 : JurisData n°2011-014804. Crim. 20 mars 2007 n°06-89.250 : JurisData n°2007-038316.
[573] V. par ex. Crim. 6 nov. 2013, n°12-87.130 : JurisData n°2013-024912 (*Op. cit.* p.35).
[574] Crim. 22 nov. 2011 n°11-84.308 : JurisData n° 2011-026053 : « […] documents issus d'un système informatique ou d'un traitement de données nominatives […]. » Il ressort de cet arrêt que la notion de système informatique au sens de l'article 77-1-1 du C. pr. pén. correspond à un espace de stockage d'informations numériques.
[575] Qui n'est autre que le support numérique d'une ou plusieurs informations.
[576] Crim. 6 mars 2013 n°12-87.810 : JurisData n°2013-004870. « La communication des bandes de vidéosurveillance issues d'un système mis en œuvre par une personne privée entre bien dans le champ d'application de l'art. 60-1 du C. pr. pén. »
BUISSON Jacques, *Perquisitions dans le parking en sous-sol d'une résidence,* JurisClasseur, Procédures n°5, Mai 2013, comm. 168.

une société privée ou à un établissement public mettant en œuvre le système de surveillance. Ce type de données ne soulève pas d'interrogation particulière.

390. Une limitation par le respect de la vie privée. – En revanche, la communication de certains fichiers en application de cette disposition peut rapidement se heurter à une intrusion trop forte dans la vie privée de la personne visée par la mesure. En effet, l'article 60-1 fait partie de la procédure de droit commun. L'obtention de données auprès d'un tiers est donc permise pour toutes les infractions[577]. De plus, cet acte peut être actionné sans aucun contrôle d'un magistrat du siège. Ainsi, il est de droit constant, au visa de l'article 8 de la Convention européenne, que toute ingérence forte dans la vie privée d'un individu ne peut être réalisée qu'avec l'autorisation et sous le contrôle d'un juge indépendant[578]. La décision du Conseil constitutionnel[579] au sujet de la loi du 23 mars 2019[580] rappelle avec insistance cette nécessité. Alors que la loi de mars 2019 tentait de créer un régime d'urgence permettant au procureur de la république d'autoriser, en autonomie, les techniques spéciales d'enquête pour une durée de 24 heures[581], le Conseil a rappelé qu'au travers de cette autorisation qui « peut se poursuivre sans contrôle ni intervention d'un magistrat du siège pendant vingt-quatre heures, le législateur a porté une atteinte inconstitutionnelle au droit au respect de la vie privée et au secret des correspondances ».

391. Or, à aucun moment les articles 60-1 et 77-1-1 ne prévoient une telle intervention, ce qui revient, de fait, à poser des limites à ces dispositions, puisque rien ne s'oppose, *a priori*, pour qu'un établissement privé, soit un prestataire de service de type hébergeur, chez qui une personne dépose des fichiers créés par cette dernière, et comportant des données personnelles sensibles. Le tiers réquisitionné peut également être un prestataire fournissant une activité de messagerie électronique. Dans de telles situations, la réquisition de ces tiers pour obtenir les informations qu'ils détiennent se heurte évidemment à une intrusion forte dans la vie privée.

---

[577] Punies d'une peine d'emprisonnement, v. C. pr. pén. art. 67.
[578] Ce que ne sont pas les magistrats du Parquet en France : CEDH 23 novembre 2010 Moulin c. France. Sur ce sujet, v. également BONIS Evelyne, *Magistrature – L'indépendance des magistrats du parquet ou le difficile exercice d'équilibriste du Conseil constitutionnel,* JurisClasseur, Droit pénal n°2, étude 3, février 2018.
[579] Conseil constitutionnel, décision n°2019-778 DC du 21 mars 2019.
[580] Loi n°2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice, *op. cit.* p.18
[581] *Ibid,* art. 46 de la loi du 23 mars 2019.

392. Une ambiguïté confirmée par la jurisprudence. – L'instabilité juridique ainsi soulevée, transparaît dans deux arrêts de la Cour de cassation. Le premier, déjà cité, du 6 novembre 2013[582], expose que des enquêteurs ont, au visa de l'article 77-1-1, demandé un certain nombre d'informations entrant dans l'extraction de traitements de données à caractère personnel[583]. Néanmoins, les enquêteurs ont été plus loin en demandant la communication du carnet d'adresses lié à la boîte mail et, surtout, la copie intégrale de cette dernière, ce qui soulève de fortes interrogations quant à l'intrusion dans la vie privée de l'individu visée par la mesure. L'arrêt rendu crée un doute majeur, puisque, d'une part, il est explicitement retenu que le fait de demander la communication « du contenu de boîtes de courriers électroniques » est « une exacte application de l'article 77-1-1 » tandis que, d'autre part, les magistrats de la chambre criminelle exposent que « hors […] le contenu des correspondances échangées, […] l'ingérence ainsi apportée dans l'exercice du droit au respect de la vie privée et familiale n'excède pas ce qui est nécessaire […] ». Techniquement, on ne peut que voir une profonde contradiction dans cette solution, car le fait de se procurer le contenu de la boîte aux lettres électronique donne évidemment accès au contenu des correspondances échangées[584].

393. Quelques semaines auparavant, l'arrêt du 22 octobre 2013[585] est relatif à une affaire où les officiers de police judiciaire, en invoquant l'article 71-1-1 au cours de l'enquête préliminaire, avaient réquisitionné un tiers pour que leur soit transmis, parmi d'autres éléments, « les contenus de tous les messages envoyés et reçus, comprenant, également les messages éliminés » d'une boîte aux lettres électronique. L'annulation fut bien évidemment demandée pour ingérence dans la vie privée en violation de l'article 8 de la Convention européenne des droits de l'homme[586]. La Cour de cassation élude la question pour rejeter le moyen, en retenant « qu'en l'absence de transcription d'un quelconque message en procédure, ce contenu n'a pas été porté à la connaissance des enquêteurs » et « qu'ainsi, il n'a pas été porté atteinte, ni à la vie privée, ni au secret des correspondances ».

---

[582] *Op. cit.* p.35. Crim. 6 nov. 2013, n°12-87.130 : v. le troisième moyen invoqué.
[583] Identification du titulaire de l'adresse mail ; adresses IP et fuseau horaire de la personne consultant le compte mail ; logs de connexion à cette adresse mail.
[584] L'accès au contenu des messages échangés est différent de l'accès à l'activité d'une ligne téléphonique : V. *supra* n°388. - Crim. 8 juillet 2015 n°15-81.731 : JurisData n°2015-016435.
[585] Crim. 22 oct. 2013, n°13-81.945 : Bull. crim. 2013, n°196 : voir, également, le troisième moyen invoqué.
[586] Au sujet de l'article 8 de la CEDH, v. *supra* n°313.

394. La limitation aux réquisitions confirmée. – Malgré le manque de clarté de ces deux décisions, on en déduit que la Cour de cassation confirme que l'accès à des correspondances privées n'est pas autorisé par les articles 60-1 et 77-1-1, ce qui est cohérent avec la position de la CJUE[587].

Au demeurant, il convient de rappeler que, pour fouiller le contenu d'une boîte aux lettres numérique, il existe des dispositions spécifiques[588].

395. Une limitation qui s'épuise au stade de l'information judiciaire. – Lorsqu'une information judiciaire est ouverte, la même réquisition en application de l'article 99-3 du Code de procédure pénale, moyennant l'autorisation expresse du juge d'instruction qui a délivré la commission rogatoire initiale, autorise la transmission des fichiers aux enquêteurs[589], qui pourront les placer sous scellés. Leur exploitation pourra alors se faire selon le régime classique d'exploitation des scellés[590].

396. L'enchaînement de ces deux actes pour procéder à des investigations au sein d'une boîte aux lettres numérique conserve un intérêt par rapport aux dispositions des articles 706-95-1 et suivants, consacrant la fouille des messageries : les investigations sont, techniquement, beaucoup plus simples à mettre en œuvre. En effet, l'obtention de la messagerie par la remise d'une copie des fichiers stockés chez le tiers réquisitionné, est un accès *offline* au contenu de cette boîte aux lettres. Cet accès est évidemment moins compliqué que la mise en œuvre de la fouille au titre de l'article 706-95-1, qui suppose de contourner le mot de passe de l'utilisateur de cette messagerie.

397. Le problème de la limitation des réquisitions au stade de l'enquête. – La prépondérance des enquêtes policières dans la recherche de la vérité au sein des procédures pénales fait que la limitation des réquisitions, qui vient d'être décrite, est un problème pour l'efficacité de l'enquête.

De plus, la mauvaise complémentarité des deux séries de dispositions qui permettent de procéder aux réquisitions, maintient cette limitation.

---

[587] CJUE 2 oct. 2018, aff. C-207/16 « Ministerio Fiscal ».
[588] V. *supra* n°358. C. pr. pén. art.706-95-1 et s.
[589] DALLEST Jacques, *Un droit de réquisition consacré,* Dalloz AJ Pénal 2004 p.346 : « Le droit de réquisition aux fins de remise de documents n'était jamais discuté et contesté quand il avait pour support une commission rogatoire délivrée par un juge d'instruction. »
[590] V. *supra* n°293.

β. L'absence de complémentarité des deux séries de dispositions

398. Une différence qui souffre d'une limitation. – Le deuxième alinéa de l'article 60-2 introduit une notion supplémentaire par rapport aux articles 60-1 et 77-1-1 en permettant, sous le contrôle du juge des libertés et de la détention, que soient prises « toutes mesures propres à assurer la préservation […] du contenu des informations consultées par les personnes utilisatrices des services fournis par les opérateurs ». En première lecture, on pourrait voir ici la réponse aux limites soulevées par l'article 60-1 lorsque la communication d'informations se heurte à la protection de la vie privée[591], car le juge des libertés et de la détention peut prescrire, sinon l'obtention directe de données, au moins le fait que celles-ci soient conservées[592]. Cette conservation, sorte de « rétention numérique », permettrait alors que l'enquête poursuive son cours sans risque de subir la volatilité des éléments numériques[593]. Ainsi, si une information judiciaire était ouverte, le juge d'instruction pourrait alors demander la communication de ces données conservées par le tiers réquisitionné, afin qu'elles soient exploitées.

399. En premier lieu, cette apparente souplesse se heurte au fait que la présente disposition vise uniquement les « opérateurs de télécommunications[594], et notamment ceux mentionnés au 1 du I de l'article 6 de la loi 2004-575 du 21 juin 2004[595] ». Ainsi, les nombreuses sociétés qui fournissent des activités de messagerie ou d'hébergement de fichiers[596], mais sans être opérateurs de télécommunications au sens légal du terme, ne peuvent être sollicités pour procéder à cette rétention des données stockées chez eux.

En second lieu, l'article 60-2 limite cette rétention au « contenu des informations consultées par les personnes utilisatrices […] ». Cela signifie que c'est uniquement le trafic, notamment le surf sur Internet, que les opérateurs de télécommunications doivent conserver en réponse à la demande des autorités judiciaires. Une messagerie électronique

[591] V. *supra* n°390.

[592] LESCLOUS Vincent, *Fasc. 20 : Enquête préliminaire - Réquisitions aux fins de remise de documents intéressant l'enquête,* Lexisexis JurisClasseur Procédure pénal, 2019 : « Ce problème de redondance partielle avec l'article 77-1-1 ne se pose pas lorsque l'article 77-1-2 est utilisé pour justifier des réquisitions aux fins de conservation de données, la conservation de documents n'étant pas prévue par l'article 77-1-1. Ce cas est soumis, par l'article 60-2, à un formalisme plus lourd que le précédent puisque l'officier de police judiciaire ne peut agir que sur réquisitions du procureur de la République, lui-même autorisé préalablement à le faire par le juge des libertés et de la détention. »

[593] V. *supra* n°223.

[594] V. Code des postes et des communications électroniques art. L32 15° : « On entend par opérateur toute personne physique ou morale exploitant un réseau de communications électroniques ouvert au public ou fournissant au public un service de communications électroniques. »

[595] « Les personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne ».

[596] Google, Microsoft, Apple, etc.

ou des fichiers hébergés chez ce même opérateur n'entrent pas dans le champ d'application du texte.

400. Une double limitation préjudiciable à l'efficacité de l'enquête. – Le fait que la demande de conservation de données se limite aux opérateurs de télécommunications et aux seules données relatives aux informations consultées est particulièrement regrettable. Si ces dispositions permettaient que le contenu de messageries électroniques, précédemment évoquées[597], ou des éléments tels que des fichiers qui seraient hébergés par un suspect chez un prestataire[598], puissent faire l'objet d'une rétention au titre de cette mesure, cela apporterait une importante efficacité à l'enquête. En effet, cela permettrait que ces données soient postérieurement obtenues par une « réquisition autorisée ». Celle-ci pourrait être actionnée, en enquête, à la suite d'une nouvelle autorisation du juge des libertés et de la détention. Elle devrait, de plus, pour être parfaitement cohérente, se limiter aux infractions relatives à la criminalité organisée.

401. Cette « réquisition autorisée », pourrait idéalement venir compléter la perquisition en ligne[599] et les investigations sur les boîtes *webmail*[600]. Au demeurant, l'efficacité qui serait ainsi apportée à l'enquête ne se ferait pas au détriment du respect des libertés individuelles, puisque ce mécanisme fonctionne en deux temps. Une première étape permettrait aux autorités judiciaires de demander à un tiers de conserver toutes les informations numériques relatives à un individu, qui sont en sa possession. La préservation de ces éléments serait ainsi garantie et accorderait un délai pour que, dans un second temps, un magistrat du siège puisse étudier la pertinence de l'analyse de ces informations.

402. Conclusion du sous-paragraphe a : la limitation du périmètre des données. – Il existe deux séries de dispositions permettant d'obtenir des informations numériques auprès de tiers. Ces deux séries de dispositions semblent, à tort, complémentaires. Ce défaut de complémentarité limite le périmètre des données susceptibles d'être réquisitionnées.

---

[597] V. *supra* n°392.
[598] Notamment en mode *cloud* : v. *supra* n°221.
[599] V. *supra* n° 250.
[600] V. *supra* n°362.

De plus, outre les incertitudes dues à ces deux séries de dispositions faussement complémentaires[601], l'obtention d'informations numériques auprès de tiers comporte une autre ambigüité. En effet, les actes permettant cette obtention ont pour finalité de permettre aux enquêteurs de fouiller les données ainsi obtenues, sans que cette fouille ne soit explicitement prévue par les textes.

b. L'autorisation de fouiller découlant de l'esprit du texte

403. L'assimilation de l'obtention et de l'exploitation. – L'objectif des articles 60-1 et 60-2 est d'obtenir des données détenues par un tiers. L'article 60-1 dispose que la personne réquisitionnée doit « remettre ces informations », et l'article 60-2 évoque « une mise à disposition les informations utiles à la manifestation de la vérité ». A aucun moment, le texte ne se prononce sur les modalités de l'exploitation des données ainsi obtenues. Il y a une sorte d'assimilation de l'exploitation et de l'obtention, le législateur ayant considéré que le fait de demander de telles données s'accompagne nécessairement de leur analyse. Cette dernière trouve sa légitimité dans les missions générales des enquêteurs telles que définies à l'article 14 du Code de procédure pénale[602], qui leur confèrent de très larges prérogatives avec, pour finalité, la manifestation de la vérité[603].

404. La limitation par le respect de la vie privée. – Pour autant, les actions les plus attentatoires aux libertés individuelles doivent être dument prévues par des actes légaux[604]. C'est pourquoi, l'ambiguïté laissée par le texte quant aux fouilles opérées sur des données obtenues par réquisition auprès de tiers, rejoint les limitations précédemment évoquées en matière de communication d'informations. Cette dernière constituerait une trop grande atteinte au respect de la vie privée[605].

405. Un objectif de cohérence dans la fouille des données. – Il est regrettable que les dispositions des articles 60-1 et 60-2 ne soient pas plus explicites, en précisant que les données envoyées par les tiers en réponse à la réquisition doivent faire l'objet d'une mise

[601] V. *supra* n°398.
[602] V. *supra* n°324.
[603] BUISSON Jacques, *Définition de la police judiciaire*, LexisNexis JurisClasseur Procédure pénale Fasc20 : « […] la police judiciaire peut finalement s'appréhender comme un instrument d'administration coercitive de la preuve au service de l'autorité judiciaire, les actes de police judiciaire ont toujours cet objet [la manifestation de la vérité judiciaire]. »
[604] Sur l'application du principe de légalité à la procédure pénale, v. DESPORTES Frédéric et LAZERGES-COUSQUER Laurence, Traité de procédure pénale, p. 141. (*op. cit.* p.35).
[605] V. *supra* n°390.

sous scellés. Cette étape aurait l'avantage de dissocier l'obtention des informations numériques et leur exploitation, qui s'intègrerait alors dans la fouille usuelle des scellés numériques[606].

406. Conclusion du sous-paragraphe A : l'obtention de données auprès de tiers. – Dans un contexte de numérisation grandissante de notre société, l'obtention de données détenues par un tiers à la procédure représente un enjeu majeur pour les autorités judiciaires. La procédure pénale prévoit que ces informations numériques puissent être demandées par le biais d'une réquisition. Malheureusement, deux séries de dispositions répondent à cet objectif, alors que leur complémentarité n'est pas claire. Par ailleurs, l'obtention de données par la réquisition se heurte au respect de la vie privée. Des adaptations des dispositions actuelles permettraient de distinguer la phase de demande de communication des informations détenues par un tiers, avec la phase de fouille des données ainsi obtenues. Cette distinction permettrait d'introduire une étape intermédiaire reposant sur une mise sous scellés, qui aurait l'avantage de laisser le temps à un juge d'ordonner la fouille de ces informations, selon des dispositions prévues pour cela.

407. Au sein des investigations numériques intrusives, l'obtention de données auprès de tiers n'est pas le seul acte d'enquête ayant pour finalité implicite la fouille d'informations numériques.

B. Le déchiffrement des données

408. La suite d'une investigation numérique antérieure. – Le décryptage[607] n'est pas une investigation numérique autonome. C'est un acte incident, dont le besoin apparaît au cours d'une investigation numérique initiale[608], qui conduit à la découverte de fichiers chiffrés. Le Code de procédure pénale retranscrit parfaitement cela : « […] lorsqu'il apparaît que des données saisies ou obtenues au cours de l'enquête ou de l'instruction ont fait l'objet d'opérations de transformation empêchant d'accéder aux informations « en clair » qu'elles contiennent ou de les comprendre, ou que ces données sont protégées par un mécanisme d'authentification […][609] ».

---

[606] V. *supra* n°293.

[607] On utilisera indifféremment les termes de chiffrement et de cryptage pour désigner « l'opération qui consiste à transformer un message […] en un autre message inintelligible pour un tiers […]. » Dans la présente étude, il s'agira bien sûr de chiffrement informatique c'est-à-dire que l'opération de cryptage est réalisée grâce à un algorithme qui vient transformer des données en des données cryptées.

[608] L'analyse d'un disque dur, d'un téléphone, une captation de données, etc.

[609] C. pr. pén. art. 230-1, 1er al.

409. La mise en œuvre du déchiffrement *(1)* prévoit plusieurs cas de figures qui en font un acte complexe pour les autorités judiciaires. Les contraintes techniques de ce type d'opération sont bien prises en considération dans les effets de la mesure *(2)*.

1. La mise en œuvre du déchiffrement

410. Un acte au sein de la procédure de droit commun. – Le déchiffrement des données fait partie de la procédure de droit commun, puisqu'il est prévu dans les « dispositions communes » applicables aussi bien en enquête qu'à l'information judiciaire[610].

411. Une étrange limitation pour les moyens de l'Etat. – Néanmoins, les autorités judiciaires compétentes[611] ne peuvent recourir aux moyens de l'Etat[612] pour procéder au déchiffrement, que si la procédure au sein de laquelle les données cryptées sont découvertes concerne des infractions pour lesquelles « la peine encourue est égale ou supérieure à deux ans d'emprisonnement[613] ».

412. Cette limitation est gênante. Dès lors que la finalité est de déchiffrer les données en question, et que ce déchiffrement est autorisé pour toutes les infractions, peu importe les moyens utilisés pour y parvenir[614] : expert, entreprise spécialisée, ou moyens de l'Etat. En conséquence, cette limitation ne trouve aucune justification dans la protection de la vie privée, qui nécessiterait de réserver une telle mesure à des infractions graves. Il semble donc que cette limitation ait plutôt été introduite par le législateur pour éviter que les moyens de l'Etat soient saisis pour les infractions les moins graves. Cette explication est dérangeante car elle sous-entend que les infractions punies de moins de deux ans d'emprisonnement ne bénéficient pas des mêmes moyens que les autres.

413. Un chevauchement avec la saisine d'un expert. – Lorsque ces dispositions propres au déchiffrement de données ont été créées[615], une précaution a été prise pour que leur mise en œuvre ne soit pas exclusive de la saisine de techniciens aptes à procéder à ce

[610] C. pr. pén. « Chapitre Ier : De la mise au clair des données chiffrées nécessaires à la manifestation de la vérité », au sein du « Titre IV : Dispositions communes » : art. 230-1 à 230-5.
[611] C. pr. pén. art. 230-1, 3ème al. : « […] le procureur de la République, la juridiction d'instruction, l'officier de police judiciaire, sur autorisation du procureur de la République ou du juge d'instruction, ou la juridiction de jugement saisie de l'affaire […] ».
[612] Sur ce que recouvre cette notion de « moyens de l'Etat », v. *infra* n°426.
[613] *Ibid.* art. 230-1
[614] V. *infra* n°422.
[615] Loi n°2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne.

décryptage, par le biais d'une réquisition ou d'une expertise[616]. En effet, la voie de la réquisition ou de la commission d'expert est explicitement conservée[617].

414. Si les autorités publiques ont pris soin de ne pas exclure le déchiffrement de données par les experts judiciaires, c'est que potentiellement, le décryptage peut être réalisé par ce biais-là. On peut alors s'interroger pourquoi cette voie procédurale pour procéder au déchiffrement des données n'était pas suffisante.

415. La contrainte des listes d'experts judiciaires. – La difficulté provient des listes d'experts[618] qui contraignent les magistrats. Le Code de procédure pénale est strict en imposant de commettre un expert inscrit sur une liste[619]. Le recours à des experts non-inscrits doit être exceptionnel et motivé[620].

416. Pour procéder au décryptage, il en résulte un manque de souplesse trop important qui poserait des difficultés pratiques, puisque les spécialistes aptes à déchiffrer des données ne sont pas nécessairement inscrits sur une liste d'experts judiciaires. En effet, ces spécialistes possèdent des compétences spécifiques et, surtout, du matériel particulier.

417. Le contrôle des spécialistes de la cryptologie. – Les autorités publiques ont identifié la nécessité de contrôler la diffusion des moyens de cryptologie sur le territoire. En effet, ces derniers sont utilisés pour rendre des informations numériques inaccessibles aux tiers. Lorsque ce tiers fait partie des autorités publiques, cela peut représenter un danger pour notre pays, tout particulièrement dans un contexte de risque terroriste[621]. C'est pourquoi les entreprises proposant la fourniture de moyens ou de prestations de cryptologie voient leurs activités contrôlées. La loi pour la confiance dans l'économie

---

[616] V. *supra* n°300.
[617] C. pr. pén art. 230-1 : « Sans préjudice des dispositions des articles 60, 77-1 et 156 […] ».
[618] V. *supra* n°301.
[619] C. pr. pén art. 157 : « Les experts sont choisis parmi les personnes physiques ou morales qui figurent sur la liste nationale dressée par la Cour de cassation ou sur une des listes dressées par les cours d'appel […]. »
[620] *Ibid.* « A titre exceptionnel, les juridictions peuvent, par décision motivée, choisir des experts ne figurant sur aucune de ces listes. »
SALATI Olivier, *Chapitre 121 – Liste nationale des experts judiciaires et listes dressées par chaque cour d'appel - Choix des experts sur ou hors des listes,* Dalloz Droit de l'expertise, 2016 : « Cette disposition [art. 157] d'ordre public étant édictée, d'après la chambre criminelle, dans l'intérêt d'une bonne administration de la justice, son inobservation par un juge d'instruction entache de nullité l'ordonnance de désignation. »
Crim. 8 juill. 2004 n°04-80.145 ; Bull. crim. n°180.
[621] V. *infra* n°433.

numérique dite LCEN[622] comporte un chapitre relatif aux « moyens et prestations de cryptologie ». Il y est prévu que l'importation[623] de moyens de cryptologie ou la fourniture de prestations de cryptage soit soumise à déclaration ou autorisation, dont le régime est précisé par un décret d'application de 2007[624].

418. L'imbrication avec l'acte de décryptage en procédure pénale. – On en déduit une certaine logique entre les dispositions du Code de procédure pénale et les obligations de déclarations et d'autorisations imposées par la LCEN. En cas de découverte de fichiers cryptés avec un matériel, un logiciel ou par un prestataire déclaré, les enquêteurs pourront saisir le prestataire, le distributeur ou l'éditeur du logiciel afin de les aider à décoder les données, puisque celui-ci est censé s'être déclaré, au titre des dispositions spécifiques prévues pour le déchiffrement des données.

419. Une prestation de serment calquée sur celle des experts. – Dans ce contexte, on comprend l'utilité des articles 230-1 et suivants pour pouvoir désigner « toute personne physique ou morale qualifiée » pour procéder au déchiffrement, sans être contraint par les listes d'experts judiciaires. Pour autant, la personne « désignée » doit prêter serment, préalablement à l'exécution des opérations de déchiffrement, comme doivent le faire les experts[625]. En effet, l'intervention technique à laquelle procède le technicien en matière de déchiffrement est assimilée aux expertises ou à une réquisition prévue aux articles 60 et 77-1. Cette assimilation est parfaitement cohérente car la personne intervenant au titre des dispositions des articles 230-1 et suivants ne se contente pas de transmettre des informations ou de réaliser un simple acte technique (comme la mise en place d'un dispositif technique nécessaire pour les écoutes téléphoniques), mais doit procéder à des opérations complexes[626].

---

[622] Loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique : Titre III : « de la sécurité dans l'économie numérique » - Chapitre Ier : « moyens et prestations de cryptologie » - art. 29 à 40

[623] L'exportation est également encadrée par cette loi, mais ce point n'intéresse pas la présente étude.

[624] Décret n°2007-663 du 2 mai 2007 pris pour l'application des articles 30, 31 et 36 de la loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique et relatif aux moyens et aux prestations de cryptologie.

[625] Voir *supra* n°301. La particularité des experts judiciaires inscrits sur la liste nationale ou l'une des listes dressées par les Cours d'appel, est que les experts prêtent serment lors de leur inscription. Si un expert non inscrit (cette situation rare car elle doit être motivée par le juge tel que le prévoit le dernier alinéa de l'art. 157 du C. pr. pén.) est commis ou réquisitionné, il doit prêter serment lors de l'acceptation de la mission : C. pr. pén. art. 160.

[626] Sur le sujet de la nécessité de la prestation de serment en fonction du type d'intervention sur les données, v. *supra* n°379.

420. Conclusion du sous-paragraphe 1 : la mise en œuvre du déchiffrement. – Les dispositions spécifiques au déchiffrement des données s'imbriquent avec la saisine d'experts judiciaires. Elles ajoutent la possibilité de confier ces opérations à des spécialistes de la cryptologie tels que les services spécialisés de l'Etat, ou de pouvoir s'adresser aux professionnels de ce secteur dont l'activité est encadrée.
Malgré cet éventail de possibilités, le déchiffrement de données n'est pas une mesure facile à exécuter lorsque celle-ci entre dans ses effets.

2. Les effets du déchiffrement

421. Deux difficultés lors de l'exécution du déchiffrement. – Les techniciens saisis pour procéder au décryptage se heurtent à des difficultés pratiques importantes *(a)*. De plus, le déchiffrement est une investigation numérique qui fait suite à un autre acte[627]. En effet, c'est lors d'un acte de fouille d'informations numériques, que les enquêteurs sont susceptibles de découvrir des données cryptées. Or, l'imbrication entre la fouille des données réalisée dans ce premier acte et la fouille des données décryptées n'est pas claire *(b)*.

a. Des difficultés techniques importantes

422. Une importante limitation technique au déchiffrement des données. – Les conditions de mise en œuvre du déchiffrement de données offrent la possibilité de pouvoir saisir des personnes compétentes en matière de cryptographie, voire des sociétés mettant en œuvre ce type de technique sur les produits qu'elles commercialisent[628]. Néanmoins, cette souplesse trouve rapidement ses limites face à la réalité technique du cryptage. En effet, la connaissance de l'algorithme et du fonctionnement du logiciel ou du matériel comportant un dispositif de chiffrement des données ne suffit pas à décoder les informations cryptées par un utilisateur de ces équipements. Le principe du chiffrement est de fonctionner avec une clé privée qui n'est connue que du seul utilisateur[629]. Ainsi, en fonction de la complexité de la clé, le déchiffrement des données peut s'avérer, dans

[627] V. *supra* n°408.
[628] V. par ex. LEMAIRE Thierry, *Gemplus veut sécuriser les extranets d'entreprise avec Gemsafe Enterprise*, Sécurité Informatique, 1 juin 2001 : « [Gemsafe Workstation] comprend une carte à puce, un lecteur et un logiciel qui offrent une protection de l'accès à l'ordinateur et au réseau, un accès sécurisé à Outlook (chiffrage des mails, authentification sur des sites Web), ainsi qu'un cryptage des fichiers sur le disque dur […]. »
[629] Il s'agit d'un mot de passe, qui génère une clé privée au sein des protocoles TLS/SSL.
V. ANSSI, *Recommandations de sécurité relatives* à TLS, 2016, p.11.

le meilleur des cas très long, voire impossible. En effet, les attaques par « force brute[630] » deviennent irréalistes en raison du nombre de combinaisons, même si elles restent très utilisées par les virus informatiques[631]. Pire, un dispositif de sécurité peut lancer un effacement automatique des données au bout d'un certain nombre de tentatives infructueuses de déverrouillage.

423. Un exemple de cette réalité a fait l'objet d'une importante médiatisation en décembre 2015, au travers de l'utilisation d'un iPhone par l'un des participants aux attentats de San Bernardino en Californie. Le FBI avait récupéré cet iPhone et son propriétaire avait activé le mécanisme de cryptage proposé par Apple sur ce produit. Cette situation a abouti à un véritable bras de fer entre les autorités américaines et Apple début 2016. L'iPhone, équipé d'un dispositif de cryptage couplé à un programme de sécurité prévoyant l'effacement automatique des données au bout de 10 tentatives échouées, empêchait le FBI de procéder à des attaques par force brute. Or, à aucun moment, il n'a été demandé à Apple de fournir le mot de passe[632] puisque seul le propriétaire du téléphone le connaissait. Ce que les autorités américaines demandaient à Apple, c'était de développer un logiciel permettant de contourner les mesures de sécurité[633], ce que la société a refusé de faire, du moins officiellement[634], au motif du respect de la vie privée des utilisateurs d'iPhone dans leur ensemble.

424. Que donnerait une telle situation en France ? – En premier lieu, on notera que le Code de procédure pénale a parfaitement intégré cette contrainte technique du risque d'effacement des données lors de l'exécution de l'acte de déchiffrement[635]. La décision d'une prise de risques pour l'intégrité des données cryptées revient aux autorités judiciaires et ne repose pas sur les techniciens procédant aux opérations.

---

[630] Une attaque par force brute consiste à créer un algorithme qui teste toutes les combinaisons de tous les caractères ASCII possibles.

[631] BOERO Alexandre, *Kaspersky a recensé 105 millions d'attaques contre des objets connectés au premier semestre*, Clubic, 17 oct. 2019 : v. pas ex. les malwares Nyadrop (« Ce malware mène une attaque par force brute sur les mots de passe (…] ») et Gafgyt (« […] Gafgyt, cible aussi les objets connectés avec 2,12 % des attaques. Il opère aussi par la force brute. »).

[632] Ce que l'on nomme la clé privée de déchiffrement : v. *supra* n°422.

[633] ROZENFED Sylvie, *Sécurité : La pomme de la discorde,* Expertises des systèmes d'information, mars 2016 n°411, p.83.
Article paru sur le site www.20minutes.fr le 17 février 2016.

[634] *In fine*, le FBI a déclaré être parvenu à accéder au contenu « sans l'aide d'Apple ». Selon une rumeur, ce serait une société Israélienne qui aurait cassé la protection mais, dans les faits, il est impossible de savoir si Apple n'a pas aidé le FBI dans la confidentialité.

[635] C. pr. pén. art. 230-2 : « En cas de risque de destruction des données ou du support physique qui les contient, l'autorisation d'altérer le support physique doit être délivrée par le procureur de la République, la juridiction d'instruction ou la juridiction de jugement saisie de l'affaire. »

Malheureusement, cette précaution n'est prise que lorsque ce sont les moyens de l'Etat qui tentent de déchiffrer les données[636]. Il est regrettable que ces dispositions ne s'appliquent pas aux techniciens saisis au titre du premier alinéa de l'article 230-1, qui ont tout autant de risques d'être confrontés à des programmes de protection déclenchant un effacement automatique des informations, que les services de l'Etat.

425. En second lieu, le législateur a opté pour une gradation particulière. Tout d'abord, les autorités judiciaires peuvent demander à une entité de décoder les fichiers. Sur ce point, l'article 230-1 prévoit, à bon escient, la possibilité de saisir une personne morale[637]. Cela paraît indispensable car, comme déjà évoqué, ce sont des sociétés éditrices de logiciels ou des fabricants de matériels qui sont le plus souvent concernés par les équipements de cryptologie. On trouve ici une nouvelle justification à la création d'une procédure distincte de la saisie d'experts judiciaires[638] puisqu'il y a très peu de personnes morales inscrites sur les listes d'experts[639].

426. Ensuite, si, comme dans le cas d'Apple[640], la structure saisie déclare son impossibilité à accomplir la mission, le législateur a prévu la possibilité d'avoir recours aux moyens de l'Etat. Il s'agit clairement des dispositifs et, surtout, du savoir-faire en cryptologie des services de renseignement et de contre-espionnage. Or, comme expliqué précédemment, les attaques par force brute ne sont pas toujours possibles ou réalistes[641].

427. On peut alors regretter que la « désignation » d'une entité pour décrypter les données ne soit assortie d'aucune mesure coercitive directement associée[642]. Certes, le Code pénal réprime lourdement le fait « pour quiconque ayant connaissance de la convention secrète de déchiffrement d'un moyen de cryptologie […] de refuser de remettre ladite convention aux autorités judiciaires ou de la mettre en œuvre […][643] ». Néanmoins, dans l'immense majorité des cas, les prestataires concernés n'ont pas connaissance de la convention secrète. C'est plus l'obligation d'apporter une assistance ou une aide technique qu'il aurait été pertinent d'encadrer.

---

[636] L'article 230-2 vise exclusivement les moyens de l'Etat.
[637] Société éditrice de logiciels de cryptographie, importateur de matériels informatiques comportant de dispositifs de chiffrement, laboratoire de recherche in informatique, etc.
[638] V. *supra* n°415.
[639] V. *supra* n°342.
[640] Qui a argué : « nous n'avons pas la clé privée, nous ne pouvons donc pas déchiffrer les données ».
[641] V. C. pr. pén. art. 230-3 qui prévoit explicitement cet échec : « […] dès qu'il apparaît que ces opérations sont techniquement impossibles […] »
[642] Cette entité ne s'expose qu'à des poursuites « classiques » et donc peu efficaces, notamment d'un point de vue temporel.
[643] C. pén. art. 434-15-2.

428. Concrètement, l'article 434-15-2 du Code pénal n'est susceptible de s'appliquer, par exemple, qu'au propriétaire du téléphone dans une situation comme celle de San Bernardino. Or, sur ce point, c'est un autre débat qui s'est ouvert en 2018 sur l'application de cette disposition. Au cours d'un procès où il était reproché à un individu d'avoir refusé de remettre, d'une part, un code permettant de décrypter des données et, d'autre part, un code activant l'accès à son téléphone, une question prioritaire de constitutionnalité a été soulevée quant à la compatibilité de l'article 434-15-2 avec le droit de se taire et de ne pas participer à sa propre incrimination. Le Conseil constitutionnel a déclaré ces dispositions conformes, sans réserve d'interprétation[644]. Faisant suite à cette décision, le tribunal correctionnel a condamné le protagoniste pour les deux refus, mais la Cour d'appel de Paris l'a relaxé pour n'avoir pas remis le code d'accès au téléphone, au motif que le code pour permettre « l'accès à un téléphone courant […] ne constitue pas une convention secrète d'un moyen de cryptologie[645] ». Cette décision est surprenante[646] puisque, comme dans le cas de l'iPhone, le code d'accès au téléphone est celui qui désactive également le cryptage du contenu de l'appareil.

429. Une faiblesse de la procédure pénale face aux prérogatives offertes en matière de renseignements. – Il apparaît ici une grande faiblesse de la procédure pénale par rapport aux moyens juridiques dont dispose l'Etat pour son activité de renseignement. En effet, le Code de la sécurité intérieure est beaucoup plus coercitif que l'article 230-1 du Code de procédure pénale, puisqu'il dispose que « les personnes physiques ou morales qui fournissent des prestations de cryptologie sont tenues de remettre […] les conventions[647] permettant le déchiffrement des données […][648] ». Le fait de ne pas déférer à ces demandes est puni de deux ans d'emprisonnement et de 150000 € d'amende[649].

430. Même si le Code de la sécurité intérieure laisse transparaitre une certaine ambiguïté en ne ciblant que les « prestataires de service de cryptologie » et pas les importateurs et éditeurs de logiciels[650], on constate à la lumière des dispositions relatives

[644] Décision n°2018-696 QPC du 30 mars 2018 du Conseil constitutionnel.
[645] CA Paris 16 avril 2019, n°19/09267.
[646] De COMBLES de NAYVES Pierre, *Le code de déverrouillage d'un téléphone n'est pas une convention de déchiffrement*, Dalloz AJ pénal 2019 p.439.
[647] La précision du C. séc. int. est ici remarquable puisque l'article R871-3 encadre ce mot en précisant que « les conventions […] s'entendent des clés cryptographiques ainsi que de tout moyen logiciel ou de toute information permettant la mise au clair des données. »
[648] C. séc. int. art. L871-1.
[649] C. séc. int. art. L871-2 et L881-2.
[650] Alors que la Loi LCEN le fait : v. *supra* n°417.

au renseignement, toute la faiblesse des procédures judiciaires au sein desquelles il y aurait un besoin impérieux d'obtenir l'aide d'un tiers technique pour déchiffrer des données.

431. Un débat de société sur la liberté de pouvoir chiffrer ses données. – La numérisation de notre société qui se traduit par, notamment, une utilisation permanente d'équipements communicants par l'immense majorité des citoyens, y compris, bien sûr, par les délinquants, fait que le sujet du chiffrement est une préoccupation actuelle importante pour les pouvoirs publics français et européens[651]. En effet, les outils de cryptage sont désormais répandus et présents sur beaucoup de terminaux mobiles. Bien sûr, on pense tout d'abord aux smartphones au travers de l'exemple de l'iPhone relaté précédemment, sans oublier que le système d'exploitation Android, le plus répandu, offre évidemment des fonctionnalités identiques. Mais cette généralisation des possibilités de chiffrer les outils numériques va au-delà des téléphones, puisque la majorité des ordinateurs portables sont désormais équipés d'une puce TPM[652] qui, lorsqu'elle est bien paramétrée, rend impossible l'analyse du disque dur[653].

432. C'est, en conséquence, un véritable débat de société qui entoure ces dispositifs de chiffrement généralisés. Nombreux, parmi les industriels de l'informatique et du numérique, sont ceux qui, dans le sillage d'Apple[654], expliquent que la possibilité de crypter le contenu d'un téléphone ou d'un ordinateur, fait partie intégrante des libertés individuelles dont tout le monde doit pouvoir disposer pour protéger ses informations personnelles[655]. Par ailleurs, le fait d'introduire une porte dérobée, autrement dit une faille de sécurité volontaire, qui permettrait aux autorités judiciaires d'accéder aux données stockées en passant outre la clé[656] choisie par l'utilisateur, représente un danger potentiel

---

[651] *Op. cit.* p.35. Conseil Justice et affaires intérieures, compte-rendu de la réunion des 8 et 9 juin 2017 : « la commission européenne a informé les ministres sur les travaux effectués dans le cadre du processus de consultation d'experts en matière de cryptage, qui devraient se poursuivre au cours des mois à venir ». Idem lors de la réunion des 12 et 13 octobre 2017.

[652] Le *Trusted Platform Module* (également nommé puce TPM) est un composant cryptographique matériel. Il est intégré sur les cartes mères des ordinateurs et autres équipements électroniques et informatiques et permet de crypter les données qui sont enregistrées sur le disque dur.

[653] V. *supra* n°294.

[654] V. *supra* n°423.

[655] Observatoire des libertés et du numérique, *Chiffrement, sécurité et libertés, positionnement de l'Observatoire*, janvier 2017 : v. le paragraphe 1 intitulé « Le chiffrement : un outil de protection des libertés. »

[656] La clé ne se limite pas à un mot de passe. En effet, avec les puces TPM dont il a été précédemment question, c'est l'empreinte digitale qui est utilisée pour accéder au contenu. La clé peut aussi être un dispositif physique tel qu'une clé USB ou un badge.

trop important car celle-ci peut être détournée de sa finalité première et exploitée par des tiers malintentionnés. Cette opinion est partagée par Guillaume POUPARD, le directeur général de l'ANSSI[657].

433. Inversement, dans le contexte généralisé de terrorisme[658] que l'on connait depuis quelques années, il peut paraître choquant que les autorités judiciaires ne puissent pas avoir accès au contenu du téléphone d'un terroriste, lorsqu'on sait à quel point il est essentiel, dans ce domaine, de pouvoir retracer le parcours d'un individu et, surtout, de retrouver les complicités dont il a pu bénéficier[659]. Ce débat de société ouvre un débat juridique des plus classiques : trouver l'équilibre entre, d'une part, la nécessité de lutter contre la criminalité et le terrorisme et le respect de la vie privée et des libertés fondamentales[660].

434. Conclusion du sous-paragraphe a : des difficultés techniques importantes. – Le déchiffrement des données est une investigation numérique qui se heurte à d'importantes difficultés techniques. Le succès pour les autorités judiciaires d'obtenir les informations intelligibles est très aléatoire, malgré la souplesse offerte aux juges ou aux enquêteurs de saisir les moyens de l'Etat en matière de renseignement.

---

[657] POUPARD Guillaume (Directeur général de l'ANSSI), *lettre du 24 mars 2016 adressée aux ministères de la Défense, de l'Économie, de l'Intérieur et de la Justice* : « L'ANSSI affirme ainsi que vouloir à tout prix garantir l'accès aux données chiffrées, par exemple au moyen d'une *backdoor*, aurait pour effet désastreux d'imposer aux concepteurs de produits et de services de sécurité un affaiblissement des mécanismes cryptographiques. Il serait d'ailleurs impossible de s'assurer que ces portes ne seront pas utilisées par des tiers. » – Au sujet de l'ANSSI : v. *supra* n°131.

[658] Sur la modification du terrorisme, v. MORVAN Patrick, *Criminologie*, 3ème édition, LexisNexis, p. 242 : « Si les attentats sont aussi anciens que le monde, il n'est pas sûr que le terrorisme contemporain ait des précédents dans la mesure où il n'est plus seulement circonscrit à certaines régions et limité à certaines périodes troublées de l'histoire d'un pays – soit un terrorisme domestique et relativement éphémère – mais aussi international, tentaculaire et durable. »

[659] CALVAR Patrick (Directeur général de la sécurité intérieure), *audition du 10 mai 2016 devant Commission de la défense nationale et des forces armées de l'Assemblée Nationale*, Compte rendu n° 47 : « Reste que nous nous heurtons à un problème bien connu et qui va grandissant : celui du chiffrement. Sans trahir le secret de l'instruction, à travers les investigations opérées à la suite des attentats de Bruxelles, nous nous sommes rendus compte que nous avions affaire à des structures très organisées, très hiérarchisées, militarisées, composées d'individus communiquant avec leur centre de commandement, demandant des instructions sur les actions à mener et, le cas échéant, des conseils techniques. Cette communication est, je le répète, permanente et aucune interception n'a été réalisée ; or même une interception n'aurait pas permis de mettre au jour les projets envisagés puisque les communications étaient chiffrées sans que personne soit capable de casser le chiffrement. Je rappellerai pour mémoire le conflit ayant opposé Apple et le Federal Bureau of Investigation (FBI) ; quand on connaît la puissance de ce dernier, on voit bien que nous sommes confrontés à un problème majeur qui dépasse largement le cadre des frontières nationales. »

[660] Convention européenne des droits de l'homme : art. 8.
V. également CEDH arrêt du 28 janvier 2003 affaire Peck c. Royaume Uni : La cour se prononce sur « la question de savoir si l'ingérence était prévue par la loi et poursuivait un but légitime. »

Lorsque les techniciens saisis parviennent à décrypter les données, l'acte de déchiffrement manque de clarté quant à la fouille des informations ainsi obtenues.

b. L'ambiguïté de la fouille au sein de l'acte de déchiffrement

435. Les contradictions au sein des dispositions du déchiffrement. – Le déchiffrement est un acte qui fait nécessairement suite à une première investigation numérique, qui a mis à jour des informations cryptées[661]. Les opérations réalisées au titre des articles 230-1 et suivants ont pour objectif de rendre intelligibles[662] ces données. Lorsque les informations décryptées sont obtenues, dans quel cadre la fouille de celles-ci est-elle permise ?

Il existe, en effet, une contradiction entre l'article 230-1 qui semble autoriser cette fouille[663] et l'article 230-3 qui suggère qu'au terme du décryptage, les informations intelligibles sont placées sous scellés et jointes au procès-verbal rendant compte des opérations effectuées[664]. Dans ce deuxième cas, la logique serait que la fouille des données déchiffrées fasse l'objet d'un nouvel acte dédié à l'exploitation des scellés[665] ou qu'elle soit exécutée au titre de l'investigation numérique initiale qui a conduit à la découverte des données cryptées.

436. Il est dommage que les dispositions relatives au déchiffrement laissent de telles ambiguïtés. Lorsque les opérations de déchiffrage sont confiées à une entreprise spécialisée dans ce domaine, ou aux moyens de l'Etat, ces entités sont totalement étrangères aux investigations et se limiteront à retourner les données décryptées. Il serait donc pertinent de prévoir une mise sous scellés systématique des informations décryptées, qui pourraient être analysées de deux manières. Si l'acte ayant conduit à la découverte des données cryptées n'est pas encore terminé, l'expert ou les enquêteurs exécutant l'investigation numérique en question sont naturellement autorisés à fouiller les données

---

[661] V. *supra* n°408.

[662] Les articles 230-1 et s. ont pour effet de rendre intelligible des données cryptées. La chambre criminelle a eu l'occasion d'affirmer que le fait de requérir une société pour rendre intelligible des informations numériques difficilement compréhensibles en raison du langage informatique utilisé (en l'occurrence XML), mais non cryptées, n'entrait pas dans le champ d'application des articles 230-1 et s.
Crim. 16 dec. 2005 n°15-82.643.

[663] C. pr. pén. art. 230-1 : « […] en vue d'effectuer les opérations techniques permettant d'obtenir l'accès à ces informations […] ».

[664] C. pr. pén. art. 230-3 : « […] les résultats sont accompagnés des indications techniques utiles à la compréhension et à leur exploitation […] » et les « éléments ainsi obtenus font l'objet d'un procès-verbal de réception et sont versés au dossier de la procédure. »

[665] V. *supra* n°293.

déchiffrées. Si cet acte est terminé, une nouvelle exploitation classique de scellés numériques peut être ordonnée[666].

437. L'évidence d'une fouille implicite. – En l'état actuel des articles 230-1 et suivants, la fouille des informations est implicitement prévue pour les personnes procédant au déchiffrement. En effet, le seul fait que la prestation de serment soit préalablement obligatoire aux opérations techniques[667], démontre que le technicien saisi est potentiellement autorisé à accéder aux contenus qui lui a été confié[668].

438. Conclusion du paragraphe §2 : les autres actes de fouille de données. – L'accès aux informations numériques générées directement ou indirectement[669] par un individu est essentiel pour les autorités judiciaires au sein d'une procédure pénale. Pourtant, outre la perquisition, peu d'actes sont explicitement prévus pour fouiller des informations numériques[670]. D'autres investigations numériques ont pour finalité de demander des données à des tiers ou de procéder à des opérations de décryptage. La fouille des informations ainsi obtenues n'est pas clairement prévue au sein des dispositions correspondantes ce qui nuit à la cohérence des investigations numériques les unes par rapport aux autres.

439. Conclusion de la section 1 : l'obtention de données par des actes de fouilles. – La procédure pénale s'est adaptée à la numérisation de notre société[671] en dématérialisant la fouille d'éléments physiques. Ainsi, des actes constituant le socle des investigations, comme la perquisition, permettant de fouiller un lieu clos telle qu'une habitation, ou la réquisition de documents papiers détenus par un tiers, ont pris en compte les informations numériques. Cette adaptation des actes permettant de fouiller des données a donc été réalisée en modifiant des mesures existantes. Il en résulte que les investigations numériques correspondantes sont éparpillées dans le Code de procédure pénale. Cet

---

666 V. *supra* n°293.
667 V. *supra* n°419.
668 La nécessité de prêter serment est un élément qui montre le degré d'intervention sur des données qu'une personne saisie peut avoir. V. *supra* n°379.
669 Dans le cas des traitements de données mis en œuvre, par exemple, par un opérateur de téléphonie mobile, les informations de géolocalisation du téléphone ne sont pas générées directement par l'utilisateur comme il le fait avec un courriel ou un SMS qu'il envoie. C'est pour cette raison qu'il convient de parler de génération indirecte de données.
670 V. *supra* n°370.
671 V. *supra* n°17.

éparpillement n'est pas, en soi, une difficulté. Le problème qui en découle est que les régimes permettant de fouiller les informations numériques ne sont pas homogènes dans les manipulations des données autorisées. Certains actes, comme la perquisition informatique[672], prennent en compte la localisation des données tandis que d'autres, comme la fouille des messageries numériques[673] ne se préoccupent pas du lieu où sont stockées les informations auxquelles les enquêteurs accèdent. Les investigations numériques sont des mesures évidemment intrusives tant les objets connectés sont le support de la vie quotidienne de tous. La majorité des actes destinés à la fouille des données s'intéressent à cette dimension. Malheureusement, ce n'est pas le cas de la réquisition de données détenues par un tiers[674] qui n'encadre pas suffisamment les informations susceptibles d'être obtenues, laissant à la jurisprudence le soin de se prononcer sur ce point. Les importantes incohérences qui en ressortent[675] contribuent à l'hétérogénéité des régimes relatifs à la fouille des données.

440. Les investigations numériques sont des actes de procédure au sein desquels des données sont recueillies ou générées au cours de son exécution et qui sont potentiellement disponibles pour la suite de l'enquête[676]. Les fouilles d'informations numériques ne sont pas les seules mesures répondant à cette définition puisque les actes de surveillance génèrent également beaucoup de données.

[672] V. *supra* n°254.
[673] V. *supra* n°358.
[674] V. *supra* n°372.
[675] V. *supra* n°392.
[676] V. *supra* n°194.

Section 2. L'obtention de données par des actes de surveillance

441. L'importance des actes de surveillance au sein de l'enquête. – La mise sous surveillance d'individus fait partie des techniques essentielles pour les enquêteurs. Elle peut consister en une simple surveillance d'un lieu public pour y observer le va-et-vient, ou à la mise sous surveillance de personnes ou d'objets[677]. L'infiltration d'un agent ou d'un militaire au cœur d'agissements délictueux ou criminels[678] constitue également une mesure de surveillance.

442. L'effet de la numérisation sur la surveillance. – Dans les années 80, la surveillance a connu une évolution technologique importante avec les écoutes téléphoniques[679]. Il s'agissait alors de dépasser la surveillance physique d'un individu pour écouter les conversations qu'il pouvait avoir avec des tiers, à distance. La numérisation de notre société a imposé une évolution supplémentaire, pour prendre en compte l'importance des données au sein de la surveillance. Deux types de données doivent être distinguées. En premier lieu, la surveillance consiste pour les enquêteurs, à espionner les données générées par un individu. La captation de données[680] est une illustration de ce type de surveillance. En second lieu, la surveillance peut consister à implanter des dispositifs spécifiques, comme avec la géolocalisation[681], qui conduit l'individu surveillé à générer des données, à son insu, qui n'auraient jamais existées sans le dispositif de surveillance[682].

443. Des investigations numériques. – L'ensemble de ces actes de surveillance sont des investigations numériques puisqu'ils conduisent à l'obtention de données[683].

444. Des actes intrusifs. – Certes, ces investigations numériques ne sont pas coercitives comme le sont les actes de fouille de données[684] telle que, par exemple, la perquisition informatique[685]. Pour autant, elles sont tout aussi intrusives dans la vie privée.

---

677 C. pr. pén. art. 706-80 et s.
678 C. pr. pén. art. 706-81 et s.
679 V. *infra* n°525.
680 V. *infra* n°570.
681 V. *infra* n°489.
682 V. *supra* n°67.
683 V. *supra* n°194.
684 V. *supra* n°243.
685 V. *supra* n°254.

445. Deux catégories d'investigations numériques dédiées à la surveillance. – Afin d'identifier l'ensemble des actes mettant en œuvre des investigations numériques dédiées à la surveillance, et d'en étudier les régimes, il convient de distinguer celles dont l'objectif se limite strictement à surveiller le comportement et les agissements d'individus *(§1)*, et celles qui, sous le couvert d'une finalité de surveillance, dépassent ce seul cadre en autorisant, de manière implicite, une certaine fouille des données *(§2)*.

§1. Des actes de stricte surveillance

446. L'observation d'espaces physiques et numériques et la surveillance des déplacements. – Les actes consacrés à une surveillance pure, c'est-à-dire sans comporter d'autres actions incidentes, autorisent deux types d'espionnage différents.

Deux mesures permettent d'observer ce qu'il se passe dans un lieu ou dans un espace numérique *(I)* tandis que la géolocalisation permet de surveiller les déplacements d'un individu *(II)*.

I – L'observation d'un lieu ou d'un espace numérique

447. Deux investigations numériques pour s'immiscer dans des échanges. – Deux investigations numériques placent l'enquêteur dans une situation d'observation. En premier lieu, la sonorisation et la fixation d'images *(A)* lui permettent de visualiser et d'écouter ce qu'il se passe dans un lieu physique au sein duquel sa présence serait rapidement détectée.

En second lieu, l'enquête sous pseudonyme *(B)* l'autorise à pénétrer un espace numérique pour y observer les échanges. Avec ce deuxième acte, une gradation supplémentaire est prévue puisque l'enquêteur peut être actif en devenant partie prenante de ces échanges.

A. La sonorisation et la fixation d'images

448. Les conditions de mise en œuvre des sonorisations et fixations d'images. – Cette investigation numérique fait partie de ce que le Code de procédure pénale nomme « les techniques spéciales d'enquête[686] ». Elles sont prévues pour la procédure dérogatoire relative à la criminalité et la délinquance organisées[687], et ne peuvent être mises en œuvre

[686] C. pr. pén. art. 706-95-11 : « Les dispositions du présent paragraphe sont applicables aux techniques spéciales d'enquête mentionnées à la présente section. »
C. pr. pén. Livre IV, Titre XXV, Chapitre II, Section 6 : Des autres techniques spéciales d'enquête.
[687] C. pr. pén. Livre IV, Titre XXV : De la procédure applicable à la criminalité et à la délinquance organisées et aux crimes.

que pour une liste d'infractions limitativement énumérées[688]. Les sonorisations et les fixations d'images font l'objet d'un paragraphe dédié au sein des techniques spéciales d'enquête[689], mais les « dispositions communes[690] » créées par la loi du 23 mars 2019[691] leurs sont applicables. Ce sont ces dernières qui précisent les infractions pour lesquelles cet acte peut être mis en œuvre, ou qui encadrent les personnes habilitées à mettre en place les dispositifs techniques nécessaires à la sonorisation ou la fixation d'images[692].

449. La différence avec les caméras mobiles. – Dans le cadre des fixations d'images, cet acte ne doit pas être confondu avec l'utilisation de caméras mobiles par les forces de l'ordre. En effet, la loi du 3 juin 2016[693] a introduit la possibilité pour les policiers et les gendarmes de pouvoir utiliser des caméras individuelles lors de « leurs missions de prévention des atteintes à l'ordre public et de protection de la sécurité des personnes et des biens ainsi que de leurs missions de police judiciaire ». Il est explicitement prévu que les enregistrements réalisés ont pour finalité, notamment, « le constat des infractions et la poursuite de leurs auteurs par la collecte de preuves[694] ». En 2018[695], l'utilisation de ces caméras individuelles a été étendue aux agents de police municipale[696] ainsi qu'aux pompiers. Dans ces deux cas, le constat et la poursuite des infractions grâce aux enregistrements sont également prévus.

450. La consultation des vidéos ainsi réalisées peut, selon les circonstances, constituer une investigation numérique efficace. Pour autant, elle reste différente de la fixation d'images prévue aux articles 706- 96 et suivants car cette dernière repose sur l'utilisation de caméras espions implantées dans un lieu précis[697].

---

[688] C. pr. pén art. 706-73 à 706-74.
[689] C. pr. pén. art. 706-96 et s. – Paragraphe 3 : Des sonorisations et des fixations d'images de certains lieux ou véhicules.
[690] C. pr. pén. art.706-95-11 et s. – Paragraphe 1 : Dispositions communes.
[691] Loi n°2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice, *op. cit.* p.18.
[692] C. pr. pén. art. 706-95-17 2ème alinéa : « [seul] un agent qualifié d'un service, d'une unité ou d'un organisme placé sous l'autorité ou la tutelle du ministre de l'intérieur ou du ministre de la défense [peut être requis pour participer à l'installation technique du dispositif]. »
[693] *Op. cit.* p.23
[694] C. séc. int. art. L241-1.
[695] Loi n°2018-697 du 3 août 2018 relative à l'harmonisation de l'utilisation des caméras mobiles par les autorités de sécurité publique.
[696] C. séc. int. art. L241-2.
[697] C. pr. pén. art. 706-97 : « La décision autorisant le recours au dispositif mentionné à l'article 706-96 comporte tous les éléments permettant d'identifier les véhicules ou les lieux privés ou publics visés […]. »

451. La différence avec la vidéoprotection. – De même, l'utilisation de « caméras espions » est différente des systèmes de vidéoprotection tels que prévus par le Code de la sécurité intérieure[698]. Certes, des vidéos ou des images extraites de ces systèmes peuvent devenir des preuves dans une procédure judiciaire. Néanmoins, elles sont obtenues par d'autres actes de procédure. Soit les images ou vidéos sont communiquées par l'entité qui met en œuvre le dispositif en réponse à une réquisition[699]. Soit le disque dur du système de vidéoprotection a été mis sous scellés, par exemple lors d'une perquisition, et est exploité classiquement[700].

452. La différence de régime entre « paroles » et « images ». – L'article 706-96 opère une étrange distinction, dans les conditions de mise en œuvre, entre « la captation, la fixation, la transmission et l'enregistrement de paroles » et « la captation, la fixation, la transmission et l'enregistrement […] de l'image d'une ou de plusieurs personnes ». Tandis que ces dispositions permettent d'enregistrer les paroles prononcées aussi bien « dans des lieux ou véhicules privés ou publics », il ne s'intéresse qu'à l'enregistrement des images « dans un lieu privé ». C'est pourquoi, la jurisprudence a eu l'occasion de préciser que c'est dans l'article 81 du Code de procédure pénale que l'utilisation de caméras espions filmant un lieu public trouve sa justification[701]. Avec l'alignement des prérogatives du Procureur au stade de l'enquête avec celles du Juge d'instruction qui tend à s'opérer depuis plusieurs années[702], il est aisé d'imaginer que l'implantation de caméras espions lors d'une enquête policière pourrait, dans l'avenir, être autorisée au titre de l'article 41.

453. L'encadrement des outils nécessaires à l'acte. – Comme précédemment expliqué, il existe différents régimes pour autoriser les enquêteurs à procéder à des investigations numériques reposant sur des actions normalement interdites[703]. Dans le cas de la sonorisation et de la fixation d'images, l'article 706-98 permet aux officiers de police judiciaire de détenir des appareils initialement conçus pour commettre des atteintes

[698] C. séc. int. art. L251-1 et s.
[699] V. *supra* n°372.
[700] V. *supra* n°293.
[701] Crim. 18 juin 2019 n°18-86.421 : JurisData n°2019-010513 – MARON Albert et HAAS Marion, *Les oubliettes de la procédure,* JurisClasseur Droit pénal n°9, Septembre 2019, comm. 158.
[702] CONTE Philippe, *Le divan d'Hercule,* JurisClasseur, Droit pénal n°3, mars 2019, repère 3 : « En raison de l'accroissement continu du rôle et, consécutivement, des pouvoirs du parquet, […] le procureur de la République est désormais « l'homme le plus puissant de France ». Il peut, grâce aux enquêtes de police, chercher la vérité dans les mêmes conditions que le juge d'instruction […]. »
[703] V. *supra* n°64.

à la vie privée[704]. C'est donc l'encadrement d'outils dont la détention est, par principe, prohibée, qui est ici autorisée pour la réalisation de la mesure[705].

454. Les effets des sonorisations et fixations d'images. – Les articles 706-96 et suivants du Code de procédure pénale permettent une intrusion discrète dans un espace fermé. Néanmoins, pour pouvoir écouter ou visualiser avec discrétion ce qu'il se passe dans cet espace, il faut préalablement avoir implanté le dispositif technique le permettant[706]. Une distinction perdure ici entre les prérogatives offertes en enquête et au stade de l'information judiciaire. C'est uniquement au cours d'une instruction qu'il est possible de déroger aux horaires prévus pour la perquisition[707] auxquels se réfèrent les présentes dispositions, en vue de pénétrer dans un lieu d'habitation.

455. Une mesure complémentaire à d'autres actes. – Associées aux écoutes téléphoniques[708], les sonorisations et fixations d'images permettent une mise sous surveillance quasi-totale des échanges que peut avoir un individu puisque, d'une part, ce sont toutes les conversations échangées oralement dans des lieux ou des véhicules qui sont espionnées et, d'autre part, les conversations téléphoniques et autres messages numériques[709] transitant sur la ligne écoutée. La fixation d'images permet de prendre des photos ou de filmer, ce qui peut s'avérer plus utile que la voix pour identifier des personnes.

456. Une difficulté pour contrôler l'utilisation des informations collectées. – Tous les actes de fouille de données et de surveillance sont fortement intrusifs et doivent, à ce titre, faire l'objet d'un encadrement strict quant à l'utilisation des informations ainsi recueillies[710]. Le juge des libertés et de la détention dispose, pour contrôler la bonne exécution de cette mesure, d'un pouvoir de sanction important puisqu'il peut « ordonner

[704] C. pén. art. 226-3.
[705] V. *supra* n°65.
[706] C'est l'objet de l'art. 706-96-1 du C. pr. pén.
[707] C. pr. pén. art. 59 : « […] les perquisitions et les visites domiciliaires ne peuvent être commencées avant 6 heures et après 21 heures. »
[708] V. *infra* n°528.
[709] Messageries instantanées (« *chat* »), réseaux sociaux peuvent être interceptés dans le cadre des écoutes téléphoniques. V. *infra* n°540.
[710] C. pr. pén. art 706-95-14, au sujet de toutes les techniques d'enquête spéciales : « Les opérations ne peuvent, à peine de nullité, avoir un autre objet que la recherche et la constatation des infractions visées dans les décisions du magistrat. »

la destruction des procès-verbaux et des enregistrements effectués » s'il « estime que les opérations n'ont pas été réalisées conformément à son autorisation[711] ». Cependant, ce contrôle est très relatif car il s'opère sur les procès-verbaux versés au dossier. Or, le risque de détournement de la sonorisation et de la fixation d'images réside précisément dans l'accès que les enquêteurs peuvent avoir à des informations qui ne seraient pas actées dans le procès-verbal.

457. En effet, même si les enquêteurs doivent consigner « dans un procès-verbal qui est versé au dossier, les données enregistrées qui sont utiles à la manifestation de la vérité [et qu'aucune] séquence relative à la vie privée étrangère aux infractions visées dans les ordonnances autorisant la mesure ne peut être conservée dans le dossier de la procédure[712] », rien n'empêche celui qui observe la scène en direct sur un écran relié aux caméras ou aux micros espions, de couper l'enregistrement et de continuer à écouter ou visualiser. Les informations ainsi obtenues peuvent orienter l'enquête ou, par exemple, l'interrogatoire d'un suspect lors de sa garde à vue.

458. Pour parfaitement appréhender une utilisation détournée d'informations obtenues au travers d'une mesure de surveillance, il est utile de s'intéresser aux écoutes téléphoniques[713], qui offrent un recul plus important que d'autres investigations numériques, plus récentes. Par exemple, les écoutes téléphoniques peuvent conduire à écouter fortuitement la conversation d'un avocat[714]. On entend par écoute fortuite, l'interception de la ligne d'un individu et que, lors d'une conversation au travers de cette ligne, un avocat se retrouve écouté. La jurisprudence est constante en la matière : la conversation ne peut être retranscrite et versée à la procédure[715] que s'il existe à l'encontre de l'avocat des suspicions de son implication dans des faits pénalement répréhensibles, au moment de l'écoute[716]. Toutefois, comme le rappelle d'autres auteurs, si les enquêteurs laissent se dérouler l'écoute fortuite sans enregistrer (ou, plus vraisemblablement sans retranscrire et verser le contenu au dossier), on est dans le registre de « l'espionnage qui ne laisse pas de trace » mais qui peut aiguiller illicitement les enquêteurs[717].

---

[711] *Ibid.* 2ème al.
[712] C. pr. pén. art. 706-95-18.
[713] V. *infra* n°528.
[714] Pour le régime de la mise sur écoute d'un avocat, v. C. pr. pén. art. 100-7.
[715] C. pr. pén art. 100-5.
[716] Crim. 15 janv. 1997 n°96-83.75 : Bull. crim. 1997 n°14 – Crim 15 juin 2016 n°15-86.043 : Bull crim. 2016, n° 186.
AMBROISE-CASTEROT Coralie, *Validation européenne des écoutes téléphoniques incidentes d'avocat,* Dalloz, AJ pénal 2016 p. 427.
[717] RIBEYRE Cédric, *Les écoutes judiciaires en procédure pénale : « Ecoutes et secret professionnel des avocats : le point de vue de l'universitaire »,* Les colloques de l'ISCJ n°2, octobre 2017.

459. L'éventualité d'un détournement est parfaitement transposable à la sonorisation et la fixation d'images, comme précédemment expliqué au travers de l'exemple d'un enquêteur qui écouterait, en direct, des personnes sans retranscrire les propos échangés dans un procès-verbal.

460. Conclusion du sous-paragraphe A : la sonorisation et la fixation d'images. – La sonorisation et la fixation d'images sont des investigations numériques car elles permettent, lorsque l'acte est terminé, de verser des données au dossier de procédure[718]. Comme toute les mesures de surveillance, elle est fortement intrusive dans la vie privée. Il est très difficile d'encadrer efficacement les informations auxquelles ont réellement accès les enquêteurs lors de l'exécution de la mesure. Même si les dispositions prévoient strictement que seuls les éléments en rapport avec les faits ayant justifiés l'ouverture de la procédure peuvent être versés au dossier, il est impossible de contrôler l'utilisation des informations auxquelles ont eu accès les enquêteurs, notamment en écoutant des conversations.

461. La sonorisation et la fixation d'images permettent d'observer ce qu'il se passe dans un lieu physique. Avec la numérisation de notre société, il est nécessaire de transposer cette possibilité d'observation à un espace numérique.

B. L'enquête sous pseudonyme

462. L'observation d'un espace numérique fermé. – L'enquête sous pseudonyme permet aux enquêteurs de pouvoir pénétrer un espace numérique qui n'est pas librement accessible[719]. Son objectif premier est de pouvoir observer les échanges qui s'opèrent au sein de cet espace et, ainsi, de pouvoir recueillir des éléments utiles à l'enquête, comme la sonorisation et la fixation d'images[720] permettent de le faire dans un lieu physique. Cependant, l'enquête sous pseudonyme va plus loin que la sonorisation et la fixation d'images car, d'autres actions, postérieurement aux observations réalisées et en fonction de celles-ci, sont autorisées pour les enquêteurs.

463. Le prolongement des recherches sur Internet. – Inversement, en amont des observations susceptibles d'être réalisées dans le cadre de l'enquête sous pseudonyme,

[718] C. pr. pén. art. 706-95-18 : « Les enregistrements sont placés sous scellés fermés. »
[719] Sur la notion d'un espace numérique librement accessible, v. *supra* n°272. : La Convention de Budapest sur la cybercriminalité du 23 novembre 2001 qui précise la notion de « données informatiques stockées […] accessibles au public (source ouverte) ».
[720] V. *supra* n°448.

les enquêteurs peuvent procéder à des recherches classiques sur Internet *(1)*. Néanmoins, ces recherches trouvent rapidement leurs limites dès lors qu'il est nécessaire d'accéder à un espace numérique fermé. L'enquête sous pseudonyme permet de dépasser cette difficulté *(2)*.

1. Les recherches sur Internet comme première étape

464. La présence d'informations personnelles et nominatives sur Internet. – L'utilisation de plus en plus importante d'Internet comme source d'information est l'une des conséquences de la numérisation de notre société[721]. Cette utilisation est devenue un réflexe aussi bien dans la vie personnelle qu'au sein des activités professionnelles. Les informations recherchées peuvent être aussi bien culturelles, techniques, informatives, commerciales, que scientifiques. De plus, des informations personnelles, ciblées, peuvent être également recherchées. Les réseaux sociaux sont, sur ce point, particulièrement « bavards ». Les sociologues expliquent que « la réussite des plates-formes relationnelles [...] doit beaucoup au fait que les personnes y exposent différents traits de leur identité[722] ».

465. La recherche d'informations personnelles en enquête[723]. – Lors de recrutements par exemple, les services des ressources humaines ont pris l'habitude de rechercher sur Internet des informations sur les candidats. Au sein de la procédure pénale, les officiers de police judiciaire en font naturellement de même. Ils recherchent des éléments sur la personnalité, les agissements ou les relations d'un individu dont le nom apparaît dans leur enquête.

466. Ces recherches entrent pleinement dans les prérogatives qui sont les leurs[724]. Les informations ainsi recueillies par les enquêteurs peuvent se comparer à celles issues d'une enquête de voisinage. Il ne s'agit pas de preuves directes, mais des indications qui

[721] V. *supra* n°17.
[722] CARDON Dominique, *Réseaux sociaux de l'Internet,* Communications 2011/1 n°88, p.141-148. CASILLI Antonio, *En attendant les robots – enquête sur le travail du clic,* SEUIL, 2019.
[723] BUISSON Jacques, *Preuve – Moyens de la preuve,* Dalloz Répertoire de droit pénal et de procédure pénale, Octobre 2019 : « al. 133. Usage d'internet par la police à des fins probatoires. »
[724] Sur le pouvoir et les prérogatives des officiers de police judiciaire, v. *supra* n°324.

permettent d'aiguiller les investigations. Ces éléments peuvent être versés à la procédure sous forme d'un procès-verbal de constat ou de constatations[725].

467. Les limites des recherches dans les données en libre accès. – Toutefois, ce type de recherche sur Internet trouve rapidement ses limites, surtout lorsqu'il s'agit de collecter des preuves en bonne et due forme. Le plus souvent, lorsqu'une personne se plaint que des propos injurieux ou diffamatoires ont été tenus à son égard, ou qu'une vidéo infamante a été mise en ligne, la constatation des faits suppose que l'on accède à un espace privé sur un site, ce que l'enquêteur ne peut pas faire sans y être autorisé par un acte de procédure, puisqu'il pénètre alors dans la vie privée des personnes utilisant cet espace numérique. En effet, la création d'un compte sur le site en question afin de s'authentifier est indispensable. Parfois, dans des situations plus contraignantes encore, la constatation d'une éventuelle infraction est à effectuer au sein d'un groupe de discussion à accès restreint[726]. C'est ici que l'enquête sous pseudonyme permet de poursuivre l'enquête.

2. Un acte pour pénétrer efficacement des groupes de discussion

468. Le prolongement des recherches sur Internet. – Dès lors que des informations ne sont accessibles qu'au travers d'un accès nécessitant une authentification, l'agent ou le militaire en charge du dossier se trouve dans une impasse. Certes, une perquisition pour pénétrer dans l'espace numériquement fermé[727] ou une réquisition à l'hébergeur ou l'éditeur du site pour obtenir une copie des données[728] serait théoriquement possible, mais ces investigations sont lourdes à la fois en procédure et dans leur exécution. De plus, le temps pour les mettre en œuvre et les réaliser risque d'être incompatible avec la volatilité de l'environnement numérique qu'est Internet[729]. C'est dans ce type de situation que les dispositions relatives à l'infiltration numérique sont parfaitement adaptées, en permettant

[725] Le constat consiste à constater la commission d'une infraction ou d'un manquement à une règlementation tandis que la constatation s'inscrit dans les actes d'administration de la preuve. La finalité des constatations est de recueillir divers indices.
Ibid. BUISSON Jacques, *Preuve – Moyens de la preuve,* Dalloz Répertoire de droit pénal et de procédure pénale, Octobre 2019 : « 58. – Définition – Au pouvoir du seul OPJ, les « constatations » consistent dans l'ensemble des opérations qui, postérieures au constat, tendent à l'administration de la preuve, au recueil ou à la saisie des indices, normalement à l'aide des moyens de la police technique et scientifique. »
[726] Il s'agit du cas le plus fréquent sur les réseaux sociaux où il faut être « un ami » pour voir ce qui a été publié ou, sur un blog, avoir été invité pour participer à une discussion.
[727] V. *supra* n°250.
[728] V. *supra* n°372.
[729] V. *supra* n°223.

d'agir avec souplesse et célérité. Cette mesure apporte la solution aux limitations soulevées par la recherche d'informations sur Internet[730]. L'agent de police judiciaire va pouvoir, par exemple, créer un compte sur un forum ou un réseau social[731] et, *a minima*, procéder à des constatations.

469. Un acte profondément modifié par la loi du 23 mars 2019. – Antérieurement à la loi du 23 mars 2019[732], l'enquête sous pseudonyme faisait partie de la procédure dérogatoire relative à la criminalité et la délinquance organisées[733]. Néanmoins, cet acte était considérablement étendu à de nombreuses autres procédures dérogatoires[734]. La loi de mars 2019 a retiré cet acte de la procédure réservée aux infractions de criminalité et de délinquance organisées pour l'intégrer dans la procédure de droit commun[735], ce qui est plutôt cohérent eu égard aux nombreuses extensions qui avaient été progressivement ajoutées pour pouvoir utiliser cette mesure. Malheureusement, le fait d'avoir déplacé cette investigation numérique lui a retiré la lisibilité qui était la sienne antérieurement à la loi de mars 2019. En effet, sous l'ancien régime, elle était perçue comme le prolongement de l'infiltration physiquement réalisée par des enquêteurs, et était donc souvent appelée « infiltration numérique[736] ».

470. Le prolongement de l'infiltration classique. – En effet, l'expression « infiltration numérique » trouvait sa source dans le fait que « l'enquête sous pseudonyme » était, placée dans une section II bis[737], créée par la loi de 2014 visant à renforcer la lutte contre le terrorisme[738]. Or, cette section faisait suite à la section II qui encadrait les infiltrations « physiques » au sein d'un réseau criminel. L'enquête sous pseudonyme apparaissait alors comme le prolongement de l'infiltration physique

[730] V. *supra* n°467.
[731] Qui s'inscrit sans ambiguïté dans le cadre d'une « participation sous pseudonyme ».
[732] Loi n°2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice, *op. cit.* p.18.
[733] V. *supra* n°448.
[734] Les infractions en matière sanitaire (ancien article 706-2-2 du C. pr. pén.), les infractions en matière de traite des êtres humains, de proxénétisme ou de recours à la prostitution des mineurs (ancien art. 706-35-1 du C. pr. pén.), les infractions de nature sexuelle et de la protection des mineurs victimes (ancien art.706-47-3 du C. pr. pén.), les atteintes aux systèmes de traitement automatisé de données et les procédures spéciales d'enquête douanière : art. 67bis-1 A du Code des douanes.
[735] Désormais l'enquête sous pseudonyme fait l'objet du chapitre VII au sein des « disposition communes » (Titre IV) communes aux enquêtes et à l'information judiciaire.
[736] Jean PRADEL parle, pour sa part, de « cyber infiltration », ce qui est synonyme. PRADEL Jean, *Procédure pénale*, p. 380. *Op. cit.* p.31
[737] Du titre XXV relatif à « la procédure applicable à la criminalité et à la délinquance organisées ».
[738] Loi n°2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme.

puisqu'elle était parfaitement complétée par l'infiltration numérique qui permet d'infiltrer, sur Internet, des forums, des sites de téléchargement, des réseaux sociaux, des groupes thématiques sur des messageries instantanées, etc.

471. Les conditions de mise en œuvre. – Désormais, l'enquête sous pseudonyme fait partie de la procédure de droit commun. Elle est simplement réservée à des infractions punies d'une peine d'emprisonnement, à l'identique de la perquisition informatique[739] (au sein de la perquisition) et des réquisitions d'informations numériques auprès de tiers[740].

472. Des conditions de mise en œuvre très souples. – Les officiers ou agents de police judiciaire doivent être habilités pour procéder à ce type d'opération[741]. Outre cette condition, l'infiltration numérique bénéficie d'un cadre beaucoup moins contraignant que d'autres investigations numériques qui sont soumises à l'autorisation d'un juge, comme avec les infiltrations numériques faisant partie des techniques spéciales d'enquête[742]. En effet, pour la première étape de l'enquête sous pseudonyme, consistant à observer les agissements qui se déroulent au sein d'un espace numérique[743], aucune autorisation n'est nécessaire. L'officier ou l'agent de police judiciaire peut décider de la mise en œuvre de cet acte, de sa propre initiative, dès lors qu'il agit au cours d'une enquête ou sur commission rogatoire. Certains praticiens du droit s'inquiètent de l'insuffisance d'encadrement procédural de cette mesure[744]. Ce n'est que pour dépasser la simple observation et pour mettre en œuvre des actions de la part des enquêteurs infiltrés que l'autorisation du procureur ou du juge d'instruction est préalablement nécessaire[745].

---

[739] V. *supra* n°253.
[740] V. *supra* n°372.
[741] C. pr. pén. art 230-46 : « les officiers ou agents de police judiciaire […] peuvent, s'ils sont affectés dans un service spécialisé et spécialement habilités à cette fin dans des conditions précisées par arrêté du ministre de la justice et du ministre de l'intérieur, procéder sous pseudonyme aux actes suivants […]. »
Arrêté du 21 octobre 2015 relatif à l'habilitation au sein de service spécialisés d'officiers ou agents de police judiciaire pouvant procéder aux enquêtes sous pseudonyme.
[742] Par ex. la sonorisation et fixation d'images, v. *supra* n°448.
C. pr. pén. art.706-95-12.
[743] V. *supra* n°462.
[744] DUMENIL Gabriel, *La nécessité urgente d'encadrer procéduralement la mesure de cyber-infiltration, LexisNexis*. *Op. cit.* p. 23
[745] C. pr. pén. art. 230-46 : « Après autorisation du procureur de la République ou du juge d'instruction saisi des faits, acquérir tout contenu, produit, substance, prélèvement ou service, y compris illicite, ou transmettre en réponse à une demande expresse des contenus illicites. »

473. Plusieurs incertitudes dans les effets de l'enquête sous pseudonyme. – Les conditions de mise en œuvre de l'enquête sous pseudonyme sont peu contraignantes mais, en revanche, lors de l'exécution de la mesure, deux points viennent complexifier cette apparente simplicité initiale.

474. Le silence en cas de découverte de faits incidents. – En premier lieu, une importante incertitude ressort du texte en cas de découverte de faits incidents. Alors que ce cas est explicitement prévu pour les investigations numériques faisant partie des techniques spéciales d'enquête[746], ou pour la géolocalisation[747], rien n'est défini ici. En l'absence de précision, c'est une solution jurisprudentielle qui s'applique : l'enquêteur a la possibilité d'ouvrir une enquête incidente[748]. Néanmoins, il est regrettable que l'enquête sous pseudonyme ne prévoie pas explicitement ce cas, à l'identique des autres actes, car sa finalité est de permettre aux enquêteurs de s'immiscer dans un espace d'échanges en ligne. Par voie de conséquence, elle peut fréquemment conduire à la découverte de faits différents de la saisine initiale. Le silence du texte peut favoriser le recours en nullité pour détournement de procédure[749].

475. La collecte ou la transmission de données. – En second lieu, un autre point mérite plus d'attention : l'extraction ou la transmission de données, toutes deux permises[750]. Ces deux actions doivent être étudiées séparément.

476. La collecte de données. – Pour comprendre l'extraction, il faut s'intéresser aux constats que les Huissiers de justice réalisent sur Internet, et dont la procédure technique est fortement encadrée[751]. L'infiltration numérique poursuit le même objectif qui est de collecter des éléments de preuve. En revanche, l'infiltration numérique permet aux enquêteurs, en procédure pénale, d'aller bien plus loin que les prérogatives offertes aux Huissiers. Alors que ces derniers doivent se limiter à décrire visuellement ce qu'ils voient et, au maximum, à procéder à des copies d'écrans qu'ils peuvent annexer à leur constat,

---

[746] C. pr. pén. art. 706-95-14 : « Le fait que ces opérations révèlent des infractions autres que celles visées dans l'autorisation du magistrat ne constitue pas une cause de nullité des procédures incidentes. »
[747] C. pr. pén. art. 230-37 : idem. V. *infra* n°489.
[748] Crim. 7 mai 2012 n°01-80.317 : JurisData n°2002-015312 – BUISSON Jacques, *L'officier de police judiciaire rogatoirement commis conserve ses pouvoirs propres de police judiciaire pour des faits nouveaux*, LexisNexis, Procédures n°10, Octobre 2002, comm. 192.
[749] Sur le détournement de procédure, v. *supra* n°369.
[750] *Ibid.* art. 230-46.
[751] Consigner l'adresse IP du poste à partir duquel sont réalisées les constatations, vider les caches du navigateur, vérifier qu'aucun proxy n'est sur le réseau, etc. V. la norme NF Z67-147 de Septembre 2010 : « Mode opératoire de procès-verbal de constat sur internet effectué par Huissier de justice ».

les enquêteurs peuvent procéder à des actions telles que « l'aspiration » d'un site Web[752], le téléchargement de photos et vidéos ou encore la capture d'un flux vidéo[753].

477. La transmission de données. – Si la collecte de données ne soulève pas d'interrogation particulière, la transmission de données pose beaucoup plus de difficultés. Le « 3° » de l'énumération faite à l'article 230-46 donne l'autorisation à l'agent infiltré de « transmettre, en réponse à une demande explicite, […] des contenus illicites ». Pour ce faire, le législateur a créé un régime d'irresponsabilité pénale pour les agents procédant à ces opérations[754]. Il s'agit là d'une différence avec les autres actes d'investigations numériques, qui, le plus souvent, prévoient plutôt un régime d'autorisation à commettre un acte interdit. C'est notamment le cas pour toutes les investigations qui autorisent à pénétrer dans un lieu privé pour y installer un dispositif [755].

478. La frontière ténue avec l'incitation à commettre une infraction[756]. – Signe de la sensibilité de cet acte sur ce point, le législateur a trouvé pertinent de devoir préciser « [qu'à] peine de nullités, […] les actes autorisés ne peuvent constituer une incitation à commettre ces infractions[757] ». Or, la transmission de données soulève une difficulté importante quant au contexte dans lequel ces informations sont envoyées à un tiers. A titre d'exemple, on peut imaginer un échange sur une messagerie instantanée entre l'agent infiltré et une personne aux déviances apparemment pédophiles. Si ce dernier indique à l'agent qu'il « aime les très jeunes filles » et, s'il demande à l'agent de lui transmettre des vidéos pornographiques correspondantes, l'enquêteur aiguille fatalement son correspondant vers une qualification particulière.

479. Que signifie, en effet, « très jeune fille » ? Jeunes majeures, adolescentes de 16-18 ans, mineures de 15 ans ? L'interprétation que va faire l'agent infiltré est ici déterminante. Il faut en effet rappeler que l'article 227-23 du Code pénal incrimine les

---

[752] L'aspiration consiste à télécharger le contenu du site internet. Cette aspiration d'un site Web trouve rapidement ses limites, puisque dès que celui-ci contient l'exécution de modules Javascript, l'affichage de la page n'est possible qu'en ligne. Dans ce cas, il n'y a pas d'autre solution que de réaliser des copies d'écran.

[753] Cas d'une vidéo qui n'est pas téléchargeable mais visualisable en *streaming* uniquement.

[754] C. pr. pén. art. 230-46 : « […] procéder sous pseudonyme aux actes suivants sans en être pénalement responsables ».

[755] Voir, par exemple, la captation des données informatiques (v. *infra* n°570.), visée par l'art. 226-3 du C. pén., qui évoque l'autorisation à utiliser les équipements correspondants.

[756] LEPAGE Agathe, *Enquête sous pseudonyme sur les réseaux numériques,* LexisNexis, Communication commerce électronique, avril 2018 : « Que la distinction entre, d'une part, provocation à la commission de l'infraction prohibée, et, d'autre part, provocation à la preuve, licite, soit parfois bien ténue […] ».

[757] C. pr. pén. art. 230-46, avant dernier alinéa.

« images pornographiques d'une personne dont l'aspect physique est celui d'un mineur », sauf s'il est établi que « cette personne était âgée de dix-huit ans au jour de la fixation de son image[758] ». Lorsque c'est l'agent infiltré qui transmet la vidéo, à qui incombe la charge de la preuve ? N'est-ce pas la première fois que le correspondant visualise ce type de vidéo, succombant à la tentation offerte par l'agent infiltré ?

480. Ce sont autant d'interrogations qui démontrent que la transmission de contenus illicites est particulièrement instable pour obtenir des preuves, dont la personne à qui elles seront opposées pourra invoquer que ses agissements ont été provoqués[759].

481. L'imbrication parfaite avec d'autres d'investigations numériques. – L'enquête sous pseudonyme apporte une grande efficacité aux outils de l'enquête car elle complète d'autres actes dédiés à la surveillance des échanges numériques : les interceptions de correspondances[760] et la captation de données[761].

482. En effet, lorsque l'agent numériquement infiltré rejoint, par exemple, un groupe privé[762] sur une messagerie instantanée, il se trouve dans un espace numérique où les membres du groupe échangent des correspondances[763]. Or, il n'est pas rare que deux protagonistes discutent plus particulièrement entre eux au sein de ce groupe. En termes de collecte de données, les effets sont identiques à une interception de correspondances entre ces deux individus puisque les données correspondant aux propos échangés peuvent être recueillies en application de l'article 230-46. Néanmoins, avec l'enquête sous pseudonyme, les données sont collectées par l'intermédiaire de l'agent infiltré ce qui constitue une différence majeure puisque les deux personnes en question ne peuvent pas ignorer que l'agent infiltré est là, à la différence de l'interception de correspondance au travers duquel les données des conversations sont obtenues totalement à l'insu des individus ciblés[764].

---

[758] Cette disposition a fait l'objet d'une question prioritaire de constitutionnalité, au motif qu'elle instituerait une présomption de culpabilité pour le détenteur de telles images. La cour de cassation n'a pas transmis la QPC. Crim. 22 août 2018, n°18-80.431, QPC.
V. CONTE Philippe, *Minorité du sujet de l'image pornographique,* JurisClasseur, Droit pénal n°12, Décembre 2018.

[759] Ass. plén. 9 déc. 2019, n°18-86.797. ECLI:FR:CCASS:2019:AP00650.

[760] V. *infra* n°528.

[761] V. *infra* n° 570.

[762] C'est-à-dire un groupe de discussion, d'échange ou même un forum dans lequel il faut être invité par les autres participants pour y participer.

[763] V. *supra* n°468.

[764] Interceptions de correspondances prévues aux articles 100 et s. du C. pr. pén. et étendu à l'enquête pour la procédure applicable à la criminalité et à la délinquance organisée par l'art. 706-95. V. *infra* n°531.

483. De même, la captation de données[765] est une mesure qui permet d'espionner des données qui seraient envoyées ou reçues par un individu et qui correspondraient à un échange de vidéo pédopornographique par exemple. Ici, les données seraient obtenues directement sur l'ordinateur de l'un des protagonistes, à son insu. Avec l'infiltration numérique, ce sont les mêmes données qui seraient collectées, mais directement dans le groupe de discussion au sein duquel la vidéo est échangée.

484. Conclusion sur sous-paragraphe B : l'enquête sous pseudonyme. – L'enquête sous pseudonyme est une infiltration numérique puisqu'elle permet de pénétrer un espace numérique pour y observer ce qu'il s'y passe. Cet acte constitue une investigation numérique car il autorise l'enquêteur qui procède à la mesure à collecter des données : il peut s'agir du contenu des échanges tenus au sein de l'espace numérique ou de télécharger des contenus illégaux mis à disposition par des tiers. Cet acte devient, toutefois, fragile dans son exécution lorsque l'enquêteur transmet un contenu illégal en réponse à une demande qu'il reçoit au sein de l'espace numérique.

485. Conclusion du sous-paragraphe I : l'observation d'un lieu ou d'un espace numérique. – La sonorisation et la fixation d'images, ainsi que l'enquête sous pseudonyme, sont des actes de procédure permettant aux enquêteurs d'observer ce qu'il se passe dans un espace physique ou numérique. Ces deux mesures aboutissent à l'obtention de données, soit issues des dispositifs de surveillance, soit extraites de l'espace numérique infiltré. Même si l'enquête sous pseudonyme permet de dépasser la seule observation, elle reste, avec la sonorisation et la fixation d'images, un acte prévu, principalement, pour surveiller.

Parmi ces mesures de stricte surveillance, elles sont accompagnées de la géolocalisation qui permet d'espionner les déplacements d'une personne ou d'un objet tel qu'un véhicule.

[765] C. pr. pén. art. 706-102-1 et s. V. *infra* n°570.

II – La géolocalisation

486. La surveillance des déplacements à distance. – La géolocalisation permet de surveiller les déplacements d'un individu, d'un véhicule ou d'un objet[766], grâce à des données émises par un dispositif technologique porté ou implanté sur l'entité surveillée[767]. La géolocalisation est une version moderne de la filature puisqu'elle permet de suivre cette entité sans mobiliser, physiquement, et en continue, des enquêteurs.

487. Plusieurs utilisations de la technique de géolocalisation en procédure pénale. – Il existe plusieurs investigations numériques dans le Code de procédure pénale, reposant sur des techniques de géolocalisation. En premier lieu, il s'agit de la géolocalisation explicitement désignée comme telle par le Code et prévue par les articles 230-32 et suivants. En second lieu, il existe une autre possibilité, pour les enquêteurs, d'obtenir et d'exploiter des données issues d'un dispositif de géolocalisation, au travers de la surveillance électronique, communément connue sous le nom de « bracelet électronique[768] ». En effet, même si le port du bracelet électronique ne s'inscrit pas dans les actes d'enquête à proprement parler, la surveillance qui en découle doit être rapprochée de la géolocalisation, non seulement en raison de sa similitude technique[769], mais également parce que, dans certaines situations, il existe des possibilités d'utilisation de ces données en enquête. L'utilisation de ces données est explicitement prévue pour des procédures pénales différentes de celle ayant conduit au placement sous surveillance électronique, ce qui en fait donc une investigation numérique.

488. En conséquence, il convient de distinguer l'étude de la géolocalisation, explicitement désignée comme telle *(A)*, de la géolocalisation qui ne porte pas son nom *(B)*.

A. La géolocalisation explicitement prévue

489. L'importance de l'outil utilisé pour géolocaliser. – Pour comprendre la géolocalisation, il est indispensable de s'intéresser aux outils techniques qui permettent

[766] C. pr. pén. art. 230-32 : « Il peut être recouru […] à la localisation en temps réel, […] d'une personne, à l'insu de celle-ci, d'un véhicule ou de tout autre objet […]. »
[767] V. par ex. la géolocalisation d'un véhicule : Crim. 7 juin 2016 n°15-87.755 : JurisData n°2016-011071 ou Crim. 2 nov. 2016 n°16-81.539 : JurisData n°2016-022750.
[768] Placement sous surveillance électronique mobile (PSEM) et le placement sous surveillance électronique (PSE) : v. *infra* n°517.
[769] Il s'agit du même type de preuve numérique qui peut en ressortir : la présence *(ou l'absence)* d'un individu à un endroit à un instant « t ».

de procéder à l'exécution de la mesure. En effet, le téléphone mobile, ou plus généralement, tout objet connecté au réseau d'un opérateur de téléphonie mobile, peut être géolocalisé. Or, plusieurs régimes existent pour accéder à ces données de géolocalisation.

Ainsi, après avoir décrit le cadre général de la géolocalisation *(1)*, il est nécessaire de d'étudier les outils techniques permettant de concrétiser les opérations de géolocalisation *(2)*.

1. Le cadre général de la géolocalisation

490. Un cadre légal récent. – La géolocalisation a fait l'objet d'une loi qui a été entièrement consacrée à cette technologie en 2014[770]. En effet, plusieurs arrêts de la Cour de cassation avaient mis en évidence le besoin impérieux d'encadrer cette technique, afin de se conformer au cadre européen en matière de respect des libertés individuelles[771]. La géolocalisation est particulièrement intrusive dans la vie privée pour la personne visée par la mesure, puisqu'elle permet de connaître, en permanence, la totalité de ses déplacements, y compris ceux qui n'ont rien à voir avec des agissements délictuels ou criminels. Il était donc indispensable de placer cet acte sous le contrôle d'un juge, ce qui n'était pas le cas avant la loi de 2014.

491. Une procédure de droit commun mais à l'utilisation limitée – Les articles résultant de la loi de 2014 font partie de la procédure de droit commun puisqu'ils sont présents dans les dispositions communes aux enquêtes et à l'information judiciaire[772]. Pour autant, l'utilisation de cette investigation numérique est limitée à des infractions punies d'au moins trois ans d'emprisonnement, pour la recherche des causes de la mort, en cas de disparition inquiétante, ou pour la recherche d'une personne en fuite[773].

[770] Loi n°2014-372 du 28 mars 2014 relative à la géolocalisation.
[771] Crim. 22 oct. 2013, n°13-81.949 : Bul. Crim. 2013 n°197 et Crim. 22 oct. 2013, n°13-81.945 : Bull. crim. 2013, n°196.
LAURENT Benoît, ROTH Cyril, BARBIER Gildas, LABROUSSE Pascale, *Géolocalisation par suivi dynamique du téléphone portable : conditions de licéité au regard de l'article 8 de la Convention européenne des droits de l'homme*, Recueil Dalloz, 2014 p.311.
[772] C. pr. pén. chapitre V : de la géolocalisation, art. 230-32 et s.
[773] C. pr. pén. art. 230-32

492. Un cadre légal complexe. – Les dispositions créées par la loi de 2014 ont fait l'objet de nombreux commentaires, tout particulièrement sur la complexité procédurale qu'elles génèrent et les difficultés d'application qu'elles peuvent laisser subsister[774].

493. La complexité des conditions de mise en œuvre. – La complexité provient de l'entrelacement entre deux séries de conditions. En premier lieu, les conditions de mise en œuvre sont différentes au stade de l'enquête et de l'instruction[775]. Cette différence est désormais usuelle puisque c'est notamment le cas avec toutes les techniques spéciales d'enquête[776], ou avec les écoutes téléphoniques[777]. En second lieu, viennent s'entrelacer des différences relatives aux conditions de mise en œuvre pour pénétrer dans un lieu afin d'y mettre en place le dispositif technique. Sont ainsi distingués, lieux « privés destinés ou utilisés à l'entrepôt de véhicules, fonds, valeurs, marchandises ou matériel », avec les véhicules, et enfin avec les lieux privés d'habitation[778]. Pour chaque cas, une intervention particulière du procureur, du juge d'instruction et du juge des libertés et de la détention sont prévues. La complexité pour l'officier de police judiciaire est redoutable. Il convient, en effet, de préciser que c'est à lui qu'incombe la responsabilité de mettre en place la géolocalisation[779] et donc de solliciter les autorisations correspondantes auprès des magistrats adéquats. Ces autorisations sont au nombre de deux puisque l'autorisation du recours à la géolocalisation[780] est différente de celle pour pénétrer dans le lieu ou le véhicule dans lequel doit être implanté le dispositif[781].

494. L'instabilité des conditions de mise en œuvre de la procédure d'urgence – Une autre source de complexité s'ajoute au travers de la procédure prévue dans des situations d'urgence[782]. On retrouve ici l'entrelacement des conditions de mise en œuvre pour la mesure de géolocalisation proprement dite, et les conditions d'accès à un lieu fermé. Pour tenir compte « du risque imminent de dépérissement des preuves ou d'atteinte

[774] PRONIER Julien, *Géolocalisation,* JurisClasseur Procédure pénale art. 230-32 à 230-44 Fasc. 20.
[775] C. pr. pén. art. 230-33.
[776] C. pr. pén. art. 706-95-12 et s.
[777] C. pr. pén. art. 100 et s à l'information judiciaire et art. 706-95 en enquête.
[778] C. pr. pén. art. 230-34.
[779] C. pr. pén. art. 230-32 dernier al.
[780] C. pr. pén. art. 230-33.
[781] C. pr. pén. art. 230-34. Crim. 18 juin 2019 n°18-86.421 : JurisData n°2019-010513 (box fermé dans lequel était stationné le véhicule). Crim. 23 mai 2017 n°16-87.323 : JurisData n°2017-009925 (parking d'un hôtel).
[782] C. pr. pén. art.230-35.

grave aux personnes ou aux biens[783] », l'officier de police judiciaire peut agir seul et de sa propre initiative, sauf pour s'introduire dans le lieu.

495. Il en résulte une forte instabilité de cette procédure d'urgence comme l'illustre un arrêt de novembre 2015 de la chambre criminelle[784]. Dans ce cas d'espèce, c'est la « jonction » entre une enquête préliminaire et l'ouverture d'une information judiciaire qui a soulevé un problème de nullité. Les enquêteurs ont installé un dispositif de géolocalisation en urgence de leur propre initiative alors qu'ils étaient en enquête préliminaire. Lorsque l'information judiciaire a été ouverte, le juge d'instruction dans la commission rogatoire qu'il a délivrée aux officiers de police judiciaire n'a pas fait référence à la géolocalisation, ce qui a emporté la nullité de l'opération.

496. La continuité de la complexité dans les effets de la géolocalisation. – Le mécanisme de la double autorisation « mise en œuvre de la mesure – introduction dans un lieu fermé » ne correspond pas aux exigences imposées pour l'exécution de la mesure. Alors que deux documents sont nécessaires pour les autorisations de mise en œuvre, les officiers de police judiciaire regroupent dans un seul procès-verbal « toutes les opérations de mise en place du moyen technique » ainsi que « les opérations d'enregistrement des données de localisation[785] ». En revanche, un procès-verbal distinct doit être établi pour décrire ou retranscrire « les données enregistrées qui sont utiles à la manifestation de la vérité[786] ». En conséquence, il serait pertinent de créer une correspondance logique entre les autorisations nécessaires au titre de la mise en œuvre de l'acte de géolocalisation, et les procès-verbaux attendus de la part des enquêteurs.

497. Conclusion du sous-paragraphe 1 : le cadre général de la géolocalisation. – Une telle complexité, tant dans les conditions de mise en œuvre que dans le suivi procédural de l'exécution de la mesure, qui repose en grande partie sur les officiers de police judiciaire, risque de nuire à l'utilisation de la géolocalisation par les enquêteurs.

---

[783] *Ibid.*

[784] Crim. 17 nov. 2015 n°15-84.025 : JurisData n°2015-025735.
CHAVENT-LECLÈRE Anne-Sophie, *Géolocalisation - Interprétation stricte des règles relatives à l'absence d'autorisation préalable de l'autorité judiciaire en cas d'urgence*, JurisClasseur, Procédures n° 1, Janvier 2016, comm. 26.

[785] C. pr. pén. art.230-38 : « L'officier de police judiciaire […] dresse procès-verbal de chacune des opérations de mise en place du moyen technique mentionné à l'article 230-32 et des opérations d'enregistrement des données de localisation. […] »

[786] C. pr. pén. art. 230-39 : « L'officier de police judiciaire […] décrit ou transcrit, dans un procès-verbal qui est versé au dossier, les données enregistrées […]. »

Un tel frein potentiel est dommageable car cette technique s'avère précieuse dans les dossiers de grande criminalité pour lesquels le besoin de connaître le lieu où se déroulent des opérations criminelles ou délictuelles est souvent compliqué à trouver[787].

498. Loin d'ajouter de la simplicité à une mesure redoutablement complexe, ce cadre légal se trouve perturbé par les outils permettant de procéder aux opérations de géolocalisation. En effet, des régimes différents cohabitent pour accéder aux données d'un même outil : le téléphone.

2. Les conséquences des outils techniques sur les régimes

499. Deux possibilités pour créer les données de géolocalisation. – Il existe deux manières pour procéder à des opérations de géolocalisation. En premier lieu, les enquêteurs ont la possibilité d'implanter un dispositif spécifique sur une personne, un véhicule ou tout autre objet. C'est ce qui ressort des articles 230-32 et 230-34 pris ensemble. En effet, le texte dispose « qu'il peut être recouru à tout moyen technique » et il est précisé que ce moyen technique peut être mis en place ou retiré par les enquêteurs sur l'entité appelée à être géolocalisée[788]. Dans ce cas, l'individu ou l'objet géolocalisé génère des données qui n'auraient jamais existées sans cette investigation numérique[789]. En second lieu, les articles 230-32 et suivants permettent d'accéder à des données de géolocalisation que l'utilisateur d'un objet numérique génère[790], en temps réel, lors du fonctionnement naturel de cet objet. Il s'agit généralement du téléphone mobile d'un individu.

500. Or, si le cas des dispositifs spécifiquement implantés *(a)* s'inscrit totalement dans les régimes qui viennent d'être décrits, la géolocalisation du téléphone est un cas particulier *(b)* car plusieurs régimes cohabitent pour un même appareil.

a. Les dispositifs spécifiques de géolocalisation

501. Plusieurs technologies. – Les dispositifs de géolocalisation implantés par les enquêteurs peuvent reposer sur différentes technologies. La plus performante repose sur des technologies GPS[791] puisqu'elles peuvent permettre de suivre le dispositif implanté

[787] Crim. 22 oct. 2013, n°13-81.949 : Bul. Crim. 2013 n°197 (*Op. cit.)*, Crim. 17 nov. 2015 n°15-84.025 : JurisData n°2015-025735 (*Op. cit.)*, CA Bordeaux 1er juin 2017 arrêt n°479, dossier n°17/00557.
[788] C. pr. pén. art. 230-34.
[789] V. *supra* n°67.
[790] V. *supra* n°57.
[791] Système de localisation par satellite.

en s'affranchissant des contraintes d'éloignement. Elles trouvent toutefois leur limite si l'objet ou l'individu, sur lequel le dispositif est implanté, entre dans un parking en sous-sol ou dans un tunnel. Une autre technologie peut faire appel à des ondes radio. Le dispositif implanté émet simplement un signal qu'un récepteur capte. L'inconvénient de ce système est la limitation à une zone au périmètre restreint. Ce type de dispositif est utilisé, par exemple, pour des filatures assistées par un dispositif de géolocalisation[792].

502. L'avantage de la précision. – La géolocalisation utilisant des dispositifs spécifiques présente un intérêt majeur, qu'est celui de la précision. Dans le cas d'une balise GPS, les enquêteurs recueillent des données permettant de localiser un individu ou un objet avec une précision de quelques mètres. C'est un avantage très important par rapport à la géolocalisation réalisée au travers d'un téléphone mobile[793] dont la précision est tributaire du maillage des bornes[794] des opérateurs de téléphonie ainsi que de l'exploitation qui est faite des données obtenues auprès de l'opérateur de téléphonie[795]. Ainsi, fréquemment, la géolocalisation au travers d'un téléphone se limite à donner une indication de présence à l'échelle d'un quartier en agglomération, ou au sein d'une zone de plusieurs hectares en campagne. Un tel niveau macroscopique peut se révéler insuffisant, notamment pour identifier avec précision le domicile d'un individu chez qui se rend la personne géolocalisée. De plus, il suffit à un utilisateur d'éteindre le téléphone pour que les enquêteurs ne soient plus en mesure de le localiser. Les dispositifs spécifiques de géolocalisation évitent cet écueil puisque la balise a été installée à l'insu de la personne suivie. Ce dernier ne peut donc pas éteindre le dispositif à sa guise.

503. Conclusion du sous-paragraphe a : les dispositifs spécifiques de géolocalisation. – La géolocalisation au travers de dispositifs spécifiques est celle qui est directement concernée par l'énorme complexité des différents régimes applicables qui viennent d'être commentés, tant au niveau de leurs conditions de mise en œuvre que dans l'exécution de la mesure. En effet, ces dispositifs spécifiques entrent pleinement dans le

[792] *Op. cit.* V. par ex. C. pr. pén. art. 230-34. Crim. 18 juin 2019 n°18-86.421 : JurisData n°2019-010513, Crim. 23 mai 2017 n°16-87.323 : JurisData n°2017-009925.
[793] V. *infra* n°505.
[794] *Ibid.*
[795] 01Net, *Les juges remettent en cause la géolocalisation*, 01NET, 2 oct. 2019 : « […] le logiciel de la police scandinave chargé de convertir les données fournies par les opérateurs était mal configuré, mais en plus, certains smartphones étaient associés à la mauvaise antenne relais, ce qui faussait le repérage des individus mis en cause. […] »

cadre de l'autorisation nécessaire pour implanter l'émetteur, qu'il soit GPS ou émettant des ondes radio.

504. Cette complexité est, sans doute, l'une des raisons qui font que les enquêteurs privilégient, dès qu'ils le peuvent, la géolocalisation d'un individu au travers de son téléphone portable.

b. Le cas particulier de la géolocalisation du téléphone

505. La géolocalisation par le bornage du téléphone. – Tout objet connecté[796] à un réseau de téléphonie mobile génère des données de localisation. En effet, le réseau de téléphonie mobile repose sur un maillage d'antennes relais réparties sur le territoire couvert par ce réseau. Pour fonctionner, l'objet communicant doit se connecter à l'une des antennes relais. C'est ce que l'on nomme le bornage. Les magistrats sont parfaitement familiarisés avec ce vocabulaire puisqu'ils n'hésitent pas à employer ce mot dans leurs décisions[797]. Bien évidemment, au sein des objets connectés, c'est le téléphone mobile qui intéresse le plus, potentiellement, les enquêteurs car il est le plus souvent porté en permanence par son propriétaire. Il permet donc de géolocaliser indirectement un individu.

506. L'obligation de conserver les données de géolocalisation par les opérateurs. – Malgré une décision de la CEDH prohibant « une surveillance générale des personnes *via* la collecte de leurs données qui transitent par leur téléphone[798] », cohérente avec la position de la CJUE[799], les opérateurs de communications électroniques[800] doivent toujours, en France, conserver des données « pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales[801] ». La liste des données et la durée de conservation sont précisées dans la partie règlementaire du Code des postes et des communications électroniques[802]. Les données « permettant d'identifier l'origine et la

[796] Il peut s'agir d'un ordinateur équipé d'une carte SIM, une tablette, ou tout autre objet communicant.
[797] CA Bordeaux 1er juin 2017 arrêt n°479, dossier n°17/00557 : le « bornage du téléphone » est l'une des charges retenues contre le condamné.
[798] CEDH 3 avril 2007 Copland C. Royaume Uni.
[799] CJUE 8 avril 2014, aff. C293/12 et C594/12 « Digital Rights Irland Ltd et a. c. Minister for communications. »
[800] C. postes et com. élect. art. L.32 : « 15° Opérateur. On entend par opérateur toute personne physique ou morale exploitant un réseau de communications électroniques ouvert au public ou fournissant au public un service de communications électroniques. »
[801] C. postes et com. élect. art. L.34-1.
[802] C. postes et com. élect. art. R.10-3.

localisation de la communication » font partie de cette liste : elles doivent être conservées un an, voire plus à la demande des autorités judiciaires[803].

507. La distinction entre « temps réel » et *« a posteriori ».* – En conséquence, on peut distinguer deux catégories de données de géolocalisation générées par le téléphone : celles qui le sont en temps réel et celles qui sont collectées et stockées par les opérateurs de téléphonie pour se conformer aux obligations légales. Cette deuxième catégorie constitue un historique des déplacements du propriétaire du téléphone qui peut être exploité *a posteriori*.

508. Des régimes liés à la temporalité du recueil des données. – Dès lors, deux régimes très différents cohabitent en procédure pénale, pour obtenir les données de géolocalisation d'un seul et même appareil, le téléphone mobile, suivant que les enquêteurs souhaitent opérer la localisation en temps réel ou accéder à l'historique du bornage de l'appareil.

509. Le régime de la géolocalisation en temps réel. – La géolocalisation en temps réel du téléphone d'un individu entre dans le champ d'application des articles 230-32 et suivants du Code de procédure pénale relatifs à la géolocalisation[804]. Certaines observations précédemment réalisées sur la complexité des régimes applicables ne concernent pas le suivi des téléphones mobiles en temps réel. En effet, toutes les difficultés inhérentes à la pose d'un dispositif spécifique de géolocalisation sont ici évitées. Même si toutes les autres complexités développées concernent le suivi des téléphones, il est incontestable que la géolocalisation, par ce biais-là, est plus simple qu'au travers des dispositifs spécifiques, par le seul fait d'échapper à toutes les contraintes de pose et de retrait de la balise.

510. De plus, pour les enquêteurs, l'activation du suivi en temps réel d'un téléphone est fortement simplifiée, puisqu'ils ont un interlocuteur unique pour ce faire, quel que soit l'opérateur de téléphonie mobile. Il s'agit, en effet, de l'une des missions dévolues[805] à la

[803] C. postes et com. élect. art. L.34-1 III : « III. – […] il peut être différé pour une durée maximale d'un an aux opérations tendant à effacer ou à rendre anonymes certaines catégories de données techniques. »
[804] L'art. 230-32 est explicite : « Il peut être recouru à tout moyen technique destiné à la localisation en temps réel […]. »
[805] C. pr. pén. art. 230-45.

Plateforme Nationale des Interceptions Judiciaires (PNIJ)[806]. La PNIJ est, en effet, positionnée comme l'interlocutrice des enquêteurs. C'est elle qui réalise l'interface avec les opérateurs de téléphonie mobile et, elle « organise la centralisation de [l']exécution » de la mesure de géolocalisation[807].

511. Le régime de l'obtention des données de géolocalisation *a posteriori*. – Il s'agit ici, pour les enquêteurs, de pouvoir exploiter les données de géolocalisation collectées et enregistrées par les opérateurs de téléphonie mobile. L'intérêt lors d'une enquête, est de pouvoir reconstituer le trajet d'un individu ou, de pouvoir déterminer sa présence en un lieu donné à un instant précis. L'obtention, par les autorités judiciaires, de ces données, déroge aux dispositions relatives à la géolocalisation. Ces dernières font, en effet, exclusivement référence à la géolocalisation « en temps réel[808] ». L'historique du bornage d'un téléphone est obtenue dans le cadre de l'obtention de données auprès d'un tiers, à savoir par une réquisition[809]. La PNIJ est, tout comme pour la mise en place de la surveillance en temps réel, positionnée comme l'interlocutrice des autorités judiciaires[810] quel que soit l'opérateur de téléphonie mobile.

512. Le régime de l'exploitation des données de géolocalisation *a posteriori*. – L'exploitation des informations obtenues en réponse à la réquisition est effectuée dans le cadre des missions générales des enquêteurs[811]. Cette différence de régime dans l'exploitation des informations de géolocalisation, suivant qu'elles sont obtenues en temps réel ou *a posteriori*, soulève une question. En effet, les dispositions relatives à la géolocalisation en temps réel ont été créées pour prendre en compte l'aspect particulièrement intrusif de cet acte de surveillance dans la vie privée de la personne ciblée par la mesure[812]. Ainsi, la géolocalisation en temps réel se déroule selon un formalisme rigoureux. Comme précédemment expliqué[813], l'exploitation des données est strictement encadrée : un procès-verbal doit décrire « les opérations d'enregistrement des données de localisation[814] », un autre retranscrit « les données […] utiles à la

[806] La PNIJ fait l'objet de développements spécifiques : v. *infra* n°687.
[807] *Ibid.* art. 230-45.
[808] V. *supra* n°509.
[809] V. *supra* n°372. C. pr. pén. art. 60-1 et art. 60-2.
[810] L'art. 230-45 du C. pr. pén. relatif à la PNIJ fait explicitement référence aux demandes réalisées au titre de l'articles 60-2 (resp. 77-1-2 en enquête préliminaire et 99-4 à l'instruction).
[811] C. pr. pén. art. 14 – V. *supra* n°403.
[812] V. *supra* n°490.
[813] V. *supra* n°496.
[814] C. pr. pén. art.230-38.

manifestation de la vérité[815] », et « les enregistrements sont placés sous scellés fermés[816] ». Dans le cas de l'exploitation de l'historique des données de géolocalisation, rien de tel n'est prévu alors que ces informations sont aussi intrusives dans la vie privée d'un individu, puisque les enquêteurs ont accès, au travers de ces données, à tous les déplacements d'une personne pendant un an.

513. Un alignement de l'exploitation des données de géolocalisation, obtenues par le biais de la réquisition, avec celle obtenues en temps réel est une nécessité pour garantir le respect des libertés individuelles.

514. Conclusion du sous-paragraphe 2 : le cas particulier de la géolocalisation du téléphone. – Il ressort une sorte de schizophrénie pour un seul et même objet (le téléphone), utilisant la même technologie (la détection par les bornes-relais) mais avec deux régimes juridiques différents pour l'obtention et l'exploitation des mêmes données. La difficulté qui en résulte, est que la géolocalisation en temps réel d'un téléphone offre plus de garantie de protection et de respect de la vie privée pour la personne visée par la mesure de surveillance, que l'exploitation de l'historique des mêmes données obtenues *a posteriori*. Néanmoins, la procédure pénale française n'est pas la seule à posséder une double approche d'un seul et même objet, puisqu'en matière de « perquisition en ligne, le droit allemand fait une différence entre un ordinateur qui se situe dans un lieu de la sphère privée et ce même ordinateur s'il se trouve dans un lieu ouvert[817] ».

515. Conclusion du sous-paragraphe A : la géolocalisation explicitement prévue. – L'investigation numérique qui consiste à suivre les déplacements d'un individu, d'un objet ou d'un véhicule est d'une redoutable complexité depuis ses conditions de mise en œuvre jusqu'à son exécution. En effet, il existe un véritable entrelacement d'une multitude de régimes relatifs à la forme de la procédure au sein de laquelle est ordonnée la mesure, à la notion d'urgence, ainsi qu'aux conditions dans lesquelles les enquêteurs peuvent implanter et retirer le dispositif de géolocalisation. L'utilisation du suivi du téléphone portable pour géolocaliser un individu est devenue très courante en enquête.

[815] C. pr. pén. art.230-39.
[816] C. pr. pén. art.230-38.
[817] JAEGER Christian, *Enquêtes secrètes, perquisitions en ligne et conservation des données en Allemagne : un équilibre entre les intérêts de la poursuite pénale et les garanties de l'Etat de droit,* Colloque sur « les investigations numériques en procédure pénale comparée » du 5 mai 2017 au Pôle Juridique et Judiciaire de Bordeaux.

Malheureusement, une nouvelle complexité est ajoutée au travers de ce cas particulier, puisque l'obtention et l'exploitation de l'historique du bornage d'un téléphone, dérogent aux dispositions générales de la géolocalisation, alors que ce sont les mêmes données qui sont concernées.

516. La géolocalisation est le support d'autres actes au sein de la procédure pénale. Or, même si ces mesures ne font pas explicitement références à cette technologie, cette dernière contribue à fournir d'autres données de localisation potentiellement utiles à une enquête.

B. La géolocalisation sous-jacente

517. La distinction entre surveillance mobile et fixe. – En préambule, en matière de bracelet électronique[818], il existe deux régimes différents que sont le placement sous surveillance électronique mobile (PSEM)[819] et le placement sous surveillance électronique (PSE)[820].

518. La technique de la géolocalisation. – Techniquement, le bracelet électronique consiste à implanter un dispositif de géolocalisation sur un individu et à recueillir des données très proches de celles obtenues avec géolocalisation en tant qu'acte de surveillance. Ainsi, les informations collectées pourraient être potentiellement intéressantes pour l'enquête. Néanmoins, pour qu'une investigation numérique puisse reposer sur ces données, il faut que ces dernières soient légalement accessibles dans le cadre d'une enquête.

519. Le cloisonnement des données du PSE. – L'unique rôle du PSE est de déclencher une alerte lorsqu'un individu sort d'une zone, de taille restreinte tel qu'un domicile, qui lui a été imposée[821]. Ce dispositif ne présente donc pas d'intérêt dans le cadre des investigations numériques, puisqu'il est implicitement prohibé[822] de géolocaliser la personne surveillée ailleurs que dans le lieu désigné. Historiquement,

[818] DECIMA Olivier, *La rupture du bracelet électronique et l'office du juge pénal,* Recueil Dalloz 2016 p.1538.
[819] C. pén. art. 131-36-9 et s. et C. pr. pén. art. 763-13.
[820] C. pén. art. 132-26-1 et s.
[821] C. pén. art. 132-26-2 : « Le placement sous surveillance électronique emporte […] interdiction de s'absenter de son domicile ou de tout autre lieu désigné par le juge d'application des peines en dehors des périodes fixées par celui-ci. » Voir également C. pr. pén. art. 142-5 et s. : « de l'assignation à résidence avec surveillance électronique. »
[822] C. pr. pén. art. 723-8 : « Le contrôle de l'exécution de la mesure est assuré au moyen d'un procédé permettant de détecter à distance la présence ou l'absence du condamné dans le seul lieu désigné par le juge de l'application des peines pour chaque période fixée. »

l'utilisation de ce dispositif technique a été introduit pour permettre « la détention à domicile sous surveillance électronique[823] ».

520. L'accès aux données du PSEM en enquête. – Contrairement au PSE, un accès aux données de localisation du PSEM est explicitement prévu lors de l'enquête. Cet accès a été officiellement consacré par le décret du 3 mars 2016[824]. Il permet « de connaitre la localisation d'une personne, même en l'absence d'une alerte […], à la demande du procureur de la République, du juge d'instruction ou des officiers de police judiciaire […] intervenant dans le cadre […] d'une enquête ou d'une information concernant un crime ou un délit […][825] ». Cette surveillance électronique est évidemment différente de la géolocalisation « acte d'enquête ». En effet, en premier lieu, elle résulte de la décision d'une juridiction de jugement[826], du juge de l'application des peines, ou d'une décision administrative depuis 2017[827], mais surtout, le dispositif n'est pas implanté sur l'individu à son insu mais en toute connaissance de cause[828]. Il en ressort donc une imputabilité plus forte que la géolocalisation « normale », d'autant plus qu'à la différence, par exemple de géolocalisation au travers du téléphone, qui peut se prêter à un tiers, le bracelet électronique est « fixé » sur la personne. En second lieu, même si elle est une mesure de contrôle des déplacements d'un individu, elle diffère des actes d'enquête dédiés à la surveillance, car elle n'est pas exécutée à l'insu de la personne surveillée.

521. Une investigation numérique potentiellement efficace. – L'accès aux données de localisation du dispositif de surveillance électronique mobile étant autorisé pour des enquêtes, l'exploitation de ces informations est une investigation numérique potentiellement intéressante. En effet, dans une procédure, généralement distincte et postérieure à celle qui est à l'origine du placement sous surveillance électronique mobile,

---

[823] BONIS Evelyne et PELTIER Virginie, *Droit de la peine*, 3ème édition, LexisNexis, p. 650.
[824] Décret n°2016-261 du 3 mars 2016 relatif aux traitements automatisés du contrôle des personnes placées sous surveillance électronique et sous surveillance électronique mobile et modifiant le code de procédure pénale (deuxième partie : Décrets en Conseil d'Etat).
[825] C. pr. pén. art. R61-12 3°.
[826] Une juridiction de jugement peut prononcer la surveillance électronique mobile à titre de mesure de sûreté en application des articles 131-36-9 et s. du C. pén. – La liste exhaustive des cas de placement sous surveillance électronique mobile est dressée aux articles R61-12 du C. pr. pén.
[827] Loi n°2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme (*op. cit.* p.35) qui a créé l'article L228-3 dans le Code de la sécurité intérieure. V. également le décret n°2018-167 du 7 mars 2018 pris pour application de l'article 6 de la loi n° 55-385 du 3 avril 1955 relative à l'état d'urgence et de l'article L. 228-3 du code de la sécurité intérieure, et relatif au placement sous surveillance électronique mobile.
[828] Le consentement de l'intéressé est même obligatoire : v. C. pén. art. 131-36-12.

il peut être précieux pour les enquêteurs de pouvoir imputer la présence de l'individu condamné à porter le bracelet, en un lieu donné et à un instant précis. En ce sens, cette investigation numérique rejoint pleinement, dans ses effets, l'acte d'enquête qu'est la géolocalisation.

522. Conclusion du sous-paragraphe B : la géolocalisation sous-jacente. – Le bracelet électronique permet aux autorités judiciaires de contrôler les déplacements d'un individu. Il existe deux régimes différents au travers du PSE et du PSEM. Seul ce dernier, autorise un accès aux données générées au travers du dispositif pour des enquêtes distinctes des faits ayant conduit au port du bracelet. Dans le cas du PSE, cet accès n'est pas autorisé. Une telle restriction est difficile à justifier. En effet, il est dommage que le même dispositif technique qu'avec le PSEM ne soit pas utilisé pour le PSE, et que les données correspondantes ne puissent pas être consultées, au moins *a posteriori.* Cette limitation se justifie difficilement par le respect des libertés individuelles des personnes placées sous surveillance électronique, puisque le dispositif est installé avec l'accord de l'individu. De plus, cet accès aux données pour vérifier la localisation précise de la personne surveillée, pourrait être réservé à des enquêtes ouvertes pour des délits graves ou des crimes, et après autorisation d'un juge.

523. Conclusion du paragraphe §1 : des actes de stricte surveillance. – Les actes de surveillance pure, c'est-à-dire ne comportant pas des actions telles que la fouille de données, dépassant le simple espionnage, permettent d'observer ce qu'il se passe dans un lieu physique ou un espace numérique, et de suivre les déplacements d'un individu ou d'un objet. Ces mesures que sont la sonorisation et la fixation d'images, l'enquête sous pseudonyme et la géolocalisation, constituent des investigations numériques car ce sont des actes d'enquête au sein desquels des données sont obtenues. Ces actes sont éparpillés dans le Code de procédure pénale car la sonorisation et la fixation d'images font partie des techniques spéciales d'enquête prévues pour la criminalité et la délinquance organisées, tandis que les dispositions relatives à la géolocalisation sont présentes au sein des dispositions communes aux enquêtes et à l'instruction. Signe des tâtonnements et des fréquentes modifications procédurales qui concernent les investigations numériques[829], l'enquête sous pseudonyme a été déplacée des mesures réservées à la procédure pour la

[829] V. *supra* n°61.

criminalité et la délinquance organisées vers les dispositions communes[830], par la loi du 23 mars 2019. Les régimes pour la mise en œuvre et encadrant l'exécution de ces mesures de stricte surveillance, diffèrent énormément d'un acte à l'autre : les conditions de d'installation des dispositifs techniques, l'autorisation des enquêteurs, soit à commettre des actes interdits, soit à posséder des outils dont la détention est prohibée, ou encore l'encadrement des procès-verbaux que doivent rédiger les enquêteurs.

524. Cet éparpillement et cette multitude de régimes différents concernent également les actes de surveillance comportant des actions secondaires dépassant le seul espionnage.

§2. Les actes dépassant la simple surveillance

525. L'origine des écoutes téléphoniques. – Les écoutes téléphoniques sont l'illustration parfaite d'un acte dont la finalité principale est la surveillance, mais qui permet désormais une certaine fouille de données. Historiquement, la mise sur écoute d'une ligne téléphonique était une action de stricte surveillance, puisqu'il s'agissait, pour les enquêteurs, d'écouter passivement le contenu des conversations tenues sur cette ligne. Elles resteront associées à l'affaire des écoutes de l'Elysée qui s'est déroulée de 1983 à 1986 et qui s'est soldée par plusieurs condamnations[831]. Par réaction à ces évènements, une loi a créé un acte dédié à cette mesure de surveillance[832].

526. L'évolution des écoutes téléphoniques. – La numérisation de notre société a créé, dans un premier temps, des lignes de téléphones mobiles et, dans un second temps, a ouvert la possibilité que des données informatiques transitent par ces mêmes lignes. Par voie de conséquence, les écoutes téléphoniques ont dû s'adapter : les données transitant sur la ligne écoutée doivent pouvoir être interceptées, au même titre que la voix. Ainsi, désormais, cet acte dépasse la simple surveillance.

527. Le prolongement des écoutes téléphoniques. – Une autre conséquence de la numérisation de notre société, est que de nouvelles investigations numériques, conçues pour prolonger les écoutes téléphoniques dans des situations particulières, améliorant ainsi l'efficacité de l'enquête, ont été créées.

L'étude des écoutes téléphoniques *(I)* est un prérequis indispensable pour comprendre l'origine et l'intérêt de ces actes en constituant le prolongement *(II)*.

---

[830] V. *supra* n°469.

[831] Condamnations devenues définitives avec l'arrêt de la Cour de cassation du 30 septembre 2008. Sources : www.lepoint.fr et www.20minutes.fr

[832] Loi n°91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications.

I – Les écoutes téléphoniques

528. L'interception de correspondances. – L'appellation « écoute téléphonique » est désormais beaucoup trop restrictive, puisque des messages de toute sorte transitent sur la ligne écoutée[833]. Le Code de procédure pénale parle « d'interception de correspondances émises par la voie des communications électroniques[834] ».

529. Les conditions de mise en œuvre de l'interception de correspondances *(A)* est étudiée préalablement à ses effets *(B)*.

A. La mise en œuvre des écoutes téléphoniques

530. Un acte originel au sein de la procédure de droit commun. – Depuis 1991[835], cet acte fait partie de la procédure de droit commun au cours de l'information judiciaire, même s'il ne peut être mis en œuvre « qu'en matière criminelle et en matière correctionnelle, si la peine encourue est égale ou supérieure à trois ans d'emprisonnement[836] ». Ce seuil des trois ans était initialement de deux ans. Il a été porté à trois ans par la loi du 23 mars 2019[837], dans un souci d'homogénéisation[838] avec la géolocalisation[839]. Une personne qui se prétend victime d'un « délit puni d'une peine d'emprisonnement commis par la voie des communications électroniques », sur sa propre ligne, peut demander au juge d'instruction que celle-ci soit mise sur écoute[840]. L'interception de correspondances fait également partie des actes autorisés pour l'enquête ouverte dans le cadre de la recherche de personnes en fuite[841]. Les prérogatives normalement dévolues au juge d'instruction sont alors réparties entre le juge des libertés et de la détention et le procureur de la république[842].

---

[833] V. *supra* n°526.
[834] C. pr. pén. art. 100 et s.
[835] *Ibid.* Loi du 10 juillet 1991.
[836] C. pr. pén. art. 100.
[837] Loi n°2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice (*op. cit.* p.18)
[838] Sur l'intention de la loi de mars 2019 d'homogénéiser les régimes des actes d'enquête, v. *supra* n°238. V. eg. VERGES Etienne, *Réforme de la procédure pénale : une loi fleuve, pour une justice au gré des courants. (Op. cit.* p.19.)
[839] V. *supra* n°491.
[840] C. pr. pén. art. 100.
[841] C. pr. pén. art. 74-2.
[842] *Ibid.* « Ces opérations sont faites sous l'autorité et le contrôle du juge des libertés et de la détention. Pour l'application des dispositions des articles 100-3 à 100-5, les attributions confiées au juge d'instruction ou à l'officier de police judiciaire commis par lui sont exercées par le procureur de la République ou l'officier de police judiciaire requis par ce magistrat. »

531. Un acte postérieurement étendu à la procédure dérogatoire pour la criminalité organisée. – L'interception de correspondances a été étendue aux enquêtes réalisées dans le cadre de la procédure prévue pour la criminalité et la délinquance organisées en 2004[843]. Tout comme pour l'enquête ouverte pour recherche d'une personne en fuite, les prérogatives normalement dévolues au juge d'instruction sont réparties entre le juge des libertés et de la détention et le procureur de la république[844]. La présence de l'article 706-95 au sein d'une section intitulée « de l'accès à distance aux correspondances stockées par la voie des communications électroniques accessibles au moyen d'un identifiant informatique », est une incohérence. Cette dénomination se réfère incontestablement à la fouille des messageries numériques[845] qui est également présente dans cette section[846]. En revanche, elle est totalement inappropriée pour les écoutes téléphoniques puisque ces dernières ont précisément pour objectif d'intercepter des correspondances, *en live* ce qui, par définition, s'oppose au fait qu'elles soient stockées.

532. Des conditions plus limitées. – Alors qu'au stade de l'information judiciaire l'interception de correspondances peut être mise en œuvre pour « une durée maximum de quatre mois », renouvelable « dans les mêmes conditions de forme et de durée, sans que la durée totale de l'interception puisse excéder un an ou, s'il s'agit d'une infraction prévue aux articles 706-73 et 706-73-1, deux ans[847], » elle se voit limitée, en enquête, à un mois, renouvelable une seule fois pour la même durée[848].

533. Un interlocuteur unique. – Les interceptions de correspondances, qu'elles soient ordonnées à l'instruction ou en enquête, ont un point en commun avec la géolocalisation des téléphones mobiles[849]. Les autorités judiciaires ne sont pas dépendantes des différents opérateurs de téléphonie pour placer une ligne sous surveillance. En effet, la Plateforme Nationale des Interceptions Judiciaires (PNIJ)[850] a pour rôle de centraliser les demandes et de suivre l'exécution des actes correspondants[851]. Elle se positionne donc à l'interface entre les enquêteurs et les différents opérateurs.

---

[843] Loi n°2004-204 du 9 mars 2004 portant adaptation de la justice aux évolutions de la criminalité.
[844] C. pr. pén. art.706-95.
[845] V. *supra* n°358.
[846] C. pr. pén. art. 706-95-1.
[847] C. pr. pén. art. 100-2.
[848] C. pr. pén. art. 706-95.
[849] V. *supra* n°509.
[850] La PNIJ fait l'objet de développements spécifiques : v. *infra* n°687.
[851] C. pr. pén. art. 230-45.

534. L'interception d'une ligne utilisée dans un état membre de l'Union européenne. – L'ordonnance du 1er décembre 2016[852] a créé un article 100-8, également applicable aux interceptions réalisées en enquête dans le cadre de la procédure dérogatoire[853], destiné à encadrer l'information due à un Etat membre de l'Union européenne, lorsqu'une ligne téléphonique interceptée est utilisée sur le territoire celui-ci. Cette information peut être réalisée, en amont, lors de la mise en œuvre de l'interception, ou, lorsque les autorités judiciaires françaises découvrent ultérieurement que cette ligne est utilisée sur le territoire de l'Etat membre concerné, *a posteriori* alors que la mesure est déjà entrée dans ses effets.

B. Les effets des écoutes téléphoniques

535. Un acte ciblant un équipement et non un individu. – Lorsque l'interception de correspondances entre dans ses effets, c'est une ligne de téléphone qui est visée par l'acte, et non un individu[854]. Ainsi, un téléphone peut se prêter à un tiers, voire peut même être utilisé par ce tiers, à l'insu du titulaire de la ligne écoutée. Pour les autorités judiciaires, cette sorte de dissociation du titulaire de la ligne et de l'appareil qui est réellement surveillé, possède des avantages et des inconvénients. En premier lieu, il peut s'agir d'inconvénients car un suspect dont la ligne est mise sur écoute, peut volontairement contrôler l'utilisation qu'il fait de son téléphone pour induire en erreur les enquêteurs. En second lieu, cette dissociation peut être un avantage car les enquêteurs mettent souvent sur écoute des lignes appartenant à des proches d'un suspect[855], ou d'une personne en fuite[856], ce qui peut leur permettre d'écouter indirectement le protagoniste.

536. L'évolution numérique de la téléphonie. – Outre l'historique juridique des écoutes téléphoniques[857], l'évolution technologique de la téléphonie a engendré des effets très importants sur cet acte d'enquête. Au début des écoutes téléphoniques, les lignes

[852] Ordonnance n°2016-1636 du 1er décembre 2016 relative à la décision d'enquête européenne en matière pénale, transposant la directive n°2014/41/UE du Parlement européen et du Conseil du 3 avril 2014 concernant la décision d'enquête européenne en matière pénale.
[853] C. pr. pén. 706-95 : « […] Les dispositions de l'article 100-8 sont applicables aux interceptions ordonnées en application du présent article. […] »
[854] V. par ex. Crim. 3 nov. 2016 n° 15-82.191 : « […] placement sous écoute téléphonique de la ligne utilisée […]. »
[855] V. par ex. la mise sur écoute du frère du suspect, Crim. 20 nov. 2019 n°18-83.541 : JurisData n°2019-020807.
[856] V. *supra* n°530.
[857] V. *supra* n°525.

étaient analogiques[858]. La voix était donc transportée sous forme d'un signal électrique. Ainsi, la mise sur écoute consistait à « dériver » la ligne, c'est-à-dire qu'un opérateur mettait en place des câbles pour la détourner vers un enregistreur ou vers un autre combiné, écouté par les enquêteurs.

537. Le détournement du flux de données. – Désormais, les réseaux téléphoniques analogiques ont quasiment disparu et la voix est numérisée et transportée sur des réseaux digitaux. La voix est une donnée comme les autres. Ainsi, l'interception de correspondances consiste à détourner et enregistrer[859] le flux de données, de la même façon, qu'avec les lignes analogiques, la dérivation envoyait la voix vers un enregistreur.

538. Un acte de surveillance. – Dès que le détournement de ligne est mis en place, l'interception de correspondances est un acte passif, dans le sens que plus aucune action technique n'est nécessaire de la part des enquêteurs : tout le flux de données transitant sur la ligne est enregistré. C'est pourquoi les écoutes téléphoniques restent bien, prioritairement, un acte de surveillance, même si la nature des données collectées soulève des interrogations.

539. Un flou important sur la nature des données autorisées à être interceptées. – Les articles 100 à 100-8 du Code de procédure pénale parlent « d'interceptions de correspondances émises par la voie des communications électroniques ». Les « communications électroniques[860] » sont définies comme « les émissions, transmissions ou réceptions de signes, de signaux d'écrits, d'images ou de sons, par voie électromagnétique[861] ». Il est alors tentant de déduire que les interceptions réalisées en application des articles 100 et suivants autorisent la collecte de toutes les données transitant sur la ligne interceptée. Or, en téléphonie, aussi bien fixe que mobile, les abonnements associent désormais quasi-systématiquement l'échange de *data*

[858] Sur la définition d'analogique, v. *supra* n°116.
[859] L'art. 100 et l'art. 100-4 font explicitement référence à l'interception et l'enregistrement des correspondances.
[860] En 1991 (Loi n°91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications), c'est le mot « télécommunications » qui était utilisé et que l'on trouve encore parfois. Son remplacement par « communications électroniques », bien plus adapté, date de la loi n°2004-669 du 9 juillet 2004 relative aux communications électroniques et aux services de communication audiovisuelle (article 1 : « télécommunication et télécommunications sont remplacés par les mots communications électroniques »). Concernant les dispositions des art. 100 et s. du C. pr. pén., c'est la loi du 3 juin 2016 *(op. cit.* p.23*)* qui est venu « homogénéiser » le vocabulaire employé.
[861] C. des postes et des comm. élect. art. L32.

informatiques à la voix. Les smartphones, par exemple, sont communicants au travers d'Internet[862]. Est-ce que l'interception de correspondances permet le détournement, par les enquêteurs, de l'ensemble de ces données transitant sur la ligne surveillée ?

540. La limitation par le mot « correspondances ». – Dans l'esprit de la loi de 1991[863], le mot « correspondances » était central dans le texte. En effet, il s'agissait, à ce moment-là, de légaliser et d'encadrer les écoutes téléphoniques après les scandales qui avaient jalonnés les années 80[864]. Ce sont donc les échanges oraux entre deux personnes que visait la loi ayant introduit les articles 100 et suivants du Code de procédure pénale. De plus, la définition littéraire du mot « correspondance » confirme cette notion d'échange d'un message entre deux ou plusieurs personnes[865], tout comme la doctrine pénaliste[866]. Cette dernière précise que la correspondance « est une relation entre deux ou plusieurs personnes, qui se sont choisies[867] ». Cette relation repose sur une sollicitation du correspondant, même si une réponse n'est pas nécessaire pour caractériser qu'une correspondance a bien été échangée. En conséquence, l'interception de toutes les données relatives à des échanges de messages ne soulève pas de difficulté particulière. Ainsi, l'accès aux SMS[868], conversations *via* les messageries instantanées, aux courriels, aux échanges au sein de réseaux sociaux[869] s'inscrit clairement dans l'esprit du texte de 1991 et dans la notion de correspondance. Il ne s'agit ici que d'une évolution de cette dernière à de nouveaux supports de communication entre deux individus qui, au demeurant, se substituent de plus en plus aux appels vocaux.

541. A l'inverse, le mot « correspondances » s'oppose à l'interception, en application des articles 100 et suivants, de toutes les autres données transitant par la ligne surveillée, et ne constituant pas le support dématérialisé de correspondances.

542. Les données dépassant la notion de « correspondances ». – Comme précédemment indiqué[870], les abonnements de téléphonie mobile incluent, le plus

[862] Mails, surf sur Internet, synchronisation d'agendas et d'applications, réseaux sociaux, etc.
[863] *Ibid.*
[864] V. *supra* n°525.
[865] Larousse : « communication par échange de lettres, de messages. »
[866] PELTIER Virginie, *Atteintes au secret des correspondances commises par les personnes dépositaires de l'autorité publique,* JurisClasseur Pénal Code art. 432-9, Fasc. 20.
[867] *Ibid*.
[868] Lorsqu'il s'agit d'une « ligne » de téléphonie mobile.
[869] Sur les échanges possibles au sein des réseaux sociaux, v. *supra* n°365.
[870] V. *supra* n°539.

souvent, une connexion à Internet dans leurs offres. Le téléphone mobile[871] utilisant la ligne, se comporte alors comme un terminal informatique et, échange donc des données de toute nature. Il peut s'agir du surf sur Internet ou encore la synchronisation d'agendas dématérialisés. Il transite également énormément de données liées au fonctionnement purement technique des applications installées sur le smartphone[872]. En aucun cas, ces informations numériques ne peuvent être considérées comme des correspondances, puisque, ces données ne correspondent en rien à des échanges entre des personnes qui se sont choisies, et qu'elles ne sont pas non plus le support d'une sollicitation d'un destinataire précis et choisi par le propriétaire du téléphone.

543. L'interprétation extensive pour l'exécution des interceptions. – Pour autant, c'est une interprétation extensive de l'interception de correspondances qui est retenue dans la pratique. En effet, la PNIJ[873] procède à l'enregistrement de tout ce qui transite sur la ligne téléphonique surveillée, y compris les données qui n'entrent pas dans la catégorie des correspondances[874]. Les interceptions de toutes les données autres que l'enregistrement des conversations orales sont appelées, par Mireille IMBERT-QUARETTA[875], les prestations annexes. Celles-ci représentent désormais 99% des demandes effectuées à la PNIJ[876].

544. Une ambiguïté inutile. – Cet enregistrement extensif de données en application des interceptions de correspondances est récent. En conséquence, il n'existe pas encore de jurisprudence concernant l'interception et l'utilisation d'informations dépassant le cadre des correspondances au sein d'une procédure. Le fait que les pouvoirs publics aient laissé cette ambiguïté s'installer est inutile, puisqu'un nouvel acte, constituant une

[871] Ou tout autre équipement connecté à cette ligne : v. *supra* n°505.
[872] Echange de fichiers entre le terminal et un serveur, etc.
[873] V. *supra* n°533.
[874] Ceci est confirmé par Mireille IMBERT-QUARETTA, contrôleure de la PNIJ lors de l'entretien du 27 septembre 2017.
IMBERT-QUARETTA Mireille, entretien du 27 septembre 2017 : « la PNIJ n'est qu'un moyen […]. Elle enregistre donc tout ce qui est ordonné par les magistrats, communication, voix, prestations annexes, *data* etc. »
V. également *infra* n°689.
[875] *Ibid.* Mireille IMBERT-QUARETTA est contrôleure de la PNIJ (la mission de contrôleur de la PNIJ est prévue à l'art. R40-53 du C. pr. pén.).
[876] IMBERT-QUARETTA Mireille, *1er rapport d'activité, La centralisation des interceptions judiciaires,* mai 2017, p.12.

extension des interceptions de correspondances[877], a été créé pour capter les données informatiques de toute nature[878].

545. Le modèle de la géolocalisation. – Pour comprendre en quoi la difficulté résultant du périmètre des données autorisées à être collectées lors d'une interception de correspondances, pourrait simplement être évitée, il faut s'intéresser à la géolocalisation[879]. En effet, dans le cas de la géolocalisation d'un téléphone mobile[880], il est explicitement prévu que les enquêteurs mettent en œuvre cet acte en sollicitant la PNIJ[881]. L'énumération de l'article 230-45 des « réquisitions et demandes » pour lesquelles la PNIJ est compétente, dépasse nettement le seul cadre des interceptions de correspondances. En conséquence, la PNIJ est positionnée comme l'interlocutrice unique pour toutes les formes de surveillance relatives aux lignes de téléphonie mobile.

546. L'incohérence de l'absence de la captation des données. – Comme précédemment expliqué, un acte dont la finalité est la captation des données a été créé[882]. Il est incohérent que les articles 706-102-1 et suivants, relatifs à cette mesure[883], ne soient pas présents au sein de l'énumération de l'article 230-45 définissant le rôle de la PNIJ. En effet, si tel était le cas, il suffirait aux enquêteurs de viser conjointement les articles autorisant la mise œuvre de l'interception de correspondances[884] et la captation des données pour intercepter, sans aucune ambiguïté, l'intégralité des informations numériques transitant au travers de la ligne mobile surveillée. Les autorités judiciaires procèdent déjà de la sorte pour associer la géolocalisation d'un téléphone et l'écoute d'une ligne.

547. L'extension de la surveillance. – Nonobstant l'ambiguïté sur la nature des données autorisées à être interceptées au titre des articles 100 et suivants, l'évolution de cet acte dans le contexte de numérisation de notre société fait que c'est un volume

[877] V. *supra* n°527.
[878] La captation des données : c. pr. pén. art. 706-102-1 et s. – V. *infra* n°570.
[879] V. *supra* n°489.
[880] V. *supra* n°505.
[881] C. pr. pén. art. 230-45 : « […] Sauf impossibilité technique, les réquisitions et demandes adressées en application des articles 60-2, 74-2, 77-1-2 ,80-4, 99-4, 100 à 100-7, 230-32 à 230-44, 706-95 et 709-1-3 du présent code […] sont transmises par l'intermédiaire de la plate-forme nationale des interceptions judiciaires […]. ». – V. *supra* n°509.
[882] V. *supra* n°544.
[883] La captation des données fait l'objet de développements spécifiques : v. *infra* n°570.
[884] C. pr. pén. art. 100 et s. lors de l'information judiciaire ou l'art. 706-95 en enquête.

important d'informations numériques qui sont potentiellement collectées et enregistrées. Ainsi, même si les écoutes téléphoniques restent principalement un acte de surveillance[885], la question de l'exploitation de ces données se pose. Le texte ne prévoit rien sur ce point, si ce n'est que les informations interceptées et utiles à la manifestation de la vérité doivent être retranscrites et versées au dossier[886]. Pour parvenir à cette étape, en fonction du volume de données, notamment relatives aux correspondances écrites échangées au travers de la ligne écoutée, il est évident qu'une étape d'analyse de ces données est nécessaire avant leur retranscription. C'est pour cette raison que l'interception de correspondances est un acte qui, lors de son exécution, dépasse la simple surveillance d'un individu. Il comporte implicitement des opérations d'analyse des données recueillies.

548. Conclusion du sous-paragraphe I : les écoutes téléphoniques. – La numérisation de notre société a eu pour effet de transformer les écoutes téléphoniques en interception de correspondances émises par la voie des communications électroniques. Cet acte de surveillance est une investigation numérique car ce sont désormais des données qui transitent au travers de la ligne téléphonique surveillée et qui sont donc interceptées et enregistrées. Le volume de données interceptées peut s'avérer important, ce qui impose que l'interception de correspondances comporte implicitement une analyse des informations recueillies, dépassant par là-même la simple surveillance.

549. L'interception de correspondances incarne parfaitement l'incohérence dans l'imbrication et l'organisation des investigations numériques les unes par rapport aux autres[887]. Outre l'éparpillement de ces dernières dans le Code de procédure pénale[888], la différence de régime dans l'imbrication des interceptions de correspondances avec la géolocalisation d'une part, et la captation de données d'autre part, illustre cette incohérence. Alors que la PNIJ est compétente pour mettre en œuvre la géolocalisation conjointement à l'interception, la captation de données ne fait pas partie de ses prérogatives. Il s'agit d'une aberration qui a pour conséquence de créer une ambiguïté sur

[885] V. *supra* n°538.
[886] C. pr. pén. art. 100-5.
[887] V. *supra* n°83.
[888] La surveillance d'un téléphone mobile, est réalisée au travers de dispositions présentes dans le titre consacré aux juridictions d'instruction (l'interception de correspondances), dans les dispositions communes à l'enquête et à l'instruction (la géolocalisation) et dans les techniques spéciales d'enquête prévue dans le cadre de la procédure pour la criminalité et la délinquance organisées (extension de l'interception, les IMSI-catchers, etc).

la nature des données collectées au titre des interceptions. En effet, toutes les données techniques nécessaires au fonctionnement des applications, le surf sur Internet, transitant sur la ligne écoutée, n'entrent pas dans la catégorie des correspondances tandis que leur recueil fait explicitement partie de la captation des données.

550. Au demeurant, cette dernière fait partie des actes qui prolongent les effets de l'interception de correspondances.

II – Le prolongement des écoutes téléphoniques

551. L'extension de l'interception des données. – Au sein des mesures de surveillance, les interceptions de correspondances émises par la voie des communications électroniques, historiquement connues sous le nom d'écoutes téléphoniques, constituent la première étape de l'évolution technologique des mesures de surveillance[889]. Elles se sont adaptées à la numérisation de notre société en permettant désormais d'intercepter les données qui transitent sur la ligne surveillée. Pour autant, de nouveaux actes se sont révélés nécessaires pour compléter et étendre les possibilités de surveillance offertes par les écoutes téléphoniques, malgré leur prise en compte de la dématérialisation des échanges.

552. Ainsi, les IMSI-catcher *(A)* permettent, notamment, de procéder à des écoutes téléphoniques en s'affranchissant de la contrainte de l'identification d'une ligne téléphonique, et la captation des données informatiques *(B)* a pour objectif d'intercepter des informations numériques sans être tributaire d'une liaison téléphonique.

A. Les IMSI-catcher

553. La neutralisation de l'acte d'interception de correspondances. – Le contexte de numérisation de notre société n'échappe pas aux délinquants et aux criminels. Par voie de conséquence, ils sont sensibilisés au fait que les outils numériques qu'ils utilisent peuvent être surveillés par les autorités judiciaires. Ainsi, dans le cas de la téléphonie mobile, ils tentent de se protéger en multipliant l'utilisation de cartes téléphoniques prépayées[890], et en les remplaçant fréquemment[891]. L'interception de correspondances est,

[889] V. *supra* n°525.
[890] En 2018, ce sont 375 000 cartes qui ont été vendues par l'ensemble des opérateurs pour le second trimestre. ARCEP, *Observatoire des marchés des communications électroniques*, 2 août 2018.
[891] V. *supra* n°60.

dans ce cas, un acte inefficace puisque les enquêteurs sont dans l'impossibilité d'identifier l'intégralité des lignes téléphoniques utilisées par les personnes visées par une enquête[892]. Le droit Allemand a tenté de réagir à cette situation en imposant aux opérateurs de téléphonie mobile qui vendent des cartes prépayées de collecter et de conserver les informations permettant d'identifier les utilisateurs. Ces obligations ont été reconnues comme conformes avec la Convention européenne des droits de l'homme[893].

554. De telles dispositions n'existent pas en France. Néanmoins, cette collecte d'informations trouve rapidement ses limites lorsqu'il s'agit de localiser et d'écouter une ligne prépayée dans un contexte nécessitant une importante rapidité de la part des autorités judiciaires. C'est alors que les IMSI-catcher prolongent l'interception de correspondances, en conservant la finalité de surveiller des lignes téléphoniques[894], mais en s'affranchissant de la contrainte de l'identification d'une ligne déterminée.

555. Une technique issue du renseignement. – La loi ne parle pas d'IMSI-catcher mais « du recueil des données techniques de connexion et des interceptions de correspondances émises par la voie des communications électroniques[895] ». Le lien avec les interceptions de correspondances est clairement établi puisque ces deux actes se réfèrent aux « interceptions de correspondances émises par la voie des communications électroniques[896] ». Cette mesure fait partie des techniques spéciales d'enquête, réservées aux procédures applicables à la criminalité et la délinquance organisées, et est issue du renseignement[897]. C'est en 2016 qu'elle a été introduite dans le Code de procédure pénale[898].

556. Les conditions de mise en œuvre. – L'essentiel des conditions de mise en œuvre des IMSI-catcher se trouve dans les dispositions communes créées par la loi du 23 mars

---

[892] Sur la distinction entre ligne téléphonique et titulaire de la ligne, v. *supra* n°535.
[893] CEDH 30 janv. 2020 Breyer c. Allemagne.
DANIS-FATOME Anne, *Opérateurs de téléphonie mobile – Pour la CEDH, la protection des données personnelles cède devant la nécessité d'assurer la sécurité publique*, LexisNexis, Communication Commerce Electronique n°5, mai 2020.
[894] La doctrine rapproche les IMSI-catcher de l'interception des correspondances électroniques : v. DECIMA Olivier, *Terreur et métamorphose*, Recueil Dalloz, 2016, p. 1826 : « Interception des correspondances électroniques (« IMSI catchers »). »
[895] C. pr. pén. art. 706-95-20.
[896] V. *supra* n°539. - C. des postes et des comm. élect. art. L32.
[897] Introduite initialement dans le C. séc. int. à l'art. L851-6 par la loi n°2015-912 du 24 juillet 2015 relative au renseignement.
[898] Par la loi n° 2016-731 du 3 juin 2016 (*op. cit.* p.23).

2019[899]. Ces dernières définissent l'utilisation de cet acte en enquête et à l'information judiciaire. Un régime dérogatoire, venant raccourcir la durée de mise en œuvre de l'une des possibilités techniques offertes par les IMSI-catcher, est prévu[900]. Pour pouvoir comprendre cette limitation de la durée de mise en œuvre, il est nécessaire de s'intéresser aux effets de la mesure[901].

557. Le piratage du réseau de téléphonie mobile. – Les IMSI-catcher sont des dispositifs techniques qui, sans avoir peur d'employer un vocabulaire choquant au premier abord, servent à pirater le réseau de téléphonie mobile[902]. En effet, l'IMSI-catcher vient « s'insérer », dans une zone déterminée, entre les antennes relais des opérateurs de téléphonie et les téléphones des utilisateurs[903]. L'acte prévu à l'article 706-95-20 a alors trois effets distincts.

558. L'identification exhaustive des utilisateurs de lignes mobiles dans une zone géographique donnée. – En premier lieu, l'IMSI-catcher identifie l'ensemble des téléphones qui « bornent[904] » autour de lui, et c'est de cette fonctionnalité que le dispositif tire son nom. En effet, cette identification se fait à l'aide de l'identifiant unique des cartes SIM, à savoir le « International Mobile Subscriber Identity » : d'où le nom d'IMSI-catcher.

559. La géolocalisation. – En deuxième lieu, lorsqu'un téléphone borne sur l'IMSI-catcher, l'identification réalisée *via* son numéro d'IMSI est inextricablement associée à

[899] Loi n°2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice. *Op. cit.* p.18. – Sur les dispositions communes aux techniques spéciales d'enquête : v. *supra* n°35.
[900] C. pr. pén. art. 706-95-20 II. Une durée de 48H00 identique au stade de l'enquête et de l'instruction, renouvelable une fois, se substitue aux durées prévues par l'article 706-95-16 (un mois renouvelable une fois en enquête et quatre mois, renouvelable, sans que la durée totale dépasse deux ans, à l'instruction).
[901] V. *infra* n°564.
[902] QUEMENER Myriam, *Les dispositions liées au numérique de la loi du 3 juin 2016 renforçant la lutte contre le crime organisé et le terrorisme*, Dalloz IP/IT 2016 p.431 : « L'IMSI-catcher est une sorte de fausse antenne relais mobile agissant dans un rayon de quelques kilomètres, qui se substitue aux antennes des opérateurs, permettant de disposer de données émises ou reçues par les terminaux ainsi leurrés qui y sont connectés. »
[903] MJOLNES Stig and OLIMID Ruxandra, *Easy 4G/LTE IMSI Catchers for Non-Programmers*, Cornell University, 15 feb. 2017.
[904] Sur la notion de bornage, v. *supra* n°505.
C. pr. pén. art. 706-95-20 : « […] recueillir les données techniques de connexion permettant l'identification d'un terminal ou du numéro d'abonnement de son utilisateur […]. »

sa géolocalisation, selon le même mécanisme qu'avec l'acte de géolocalisation appliqué aux téléphones mobiles[905]. Cette localisation est prévue par le texte[906].

560. L'interception de correspondances. – En troisième lieu, l'IMSI-catcher peut enregistrer l'intégralité des données qui transitent au travers d'une ligne téléphonique détournée par le dispositif[907], à l'identique de ce que l'interception de correspondances prévue aux articles 100 et suivants autorisent[908].

561. La confusion avec d'autres actes aux mêmes finalités. – La deuxième et la troisième fonction de l'IMSI-catcher sont totalement identiques à deux autres investigations numériques : la géolocalisation d'un téléphone[909] et l'interception de correspondances[910]. Lorsque les autorités publiques ont introduit ces dispositions, elles ont raisonné sur l'outil technique qui permet d'exécuter la mesure et non sur la cohérence des investigations numériques les unes avec les autres. La conséquence est, une nouvelle fois[911], la création de plusieurs régimes différents pour procéder à une seule et même investigation numérique. La rigueur consisterait à opérer, au sein de l'acte encadrant les IMSI-catcher, à un renvoi vers les actes dédiés à la géolocalisation et aux interceptions de correspondances. *A contrario*, le choix a été fait de créer un acte « fourre-tout », se chevauchant avec d'autres investigations numériques, au seul motif que cet acte plus récent regroupe des fonctionnalités techniques communes à un dispositif.

562. Une collecte de données massive et générale. – Les IMSI-catcher sont particulièrement décriés par la doctrine[912], notamment en raison d'un effet qui a retenu l'attention de tous : le dispositif capte les données de tous les téléphones présents dans sa zone d'activité, sans aucun discernement. Pour autant, il existe, avec ces dispositifs, un autre point particulièrement attentatoire à la vie privée qui passe beaucoup plus inaperçu.

---

[905] V. *supra* n°505.
[906] C. pr. pén. art. 706-95-20 : « […] ainsi que les données relatives à la localisation d'un équipement terminal utilisé. »
[907] C. pr. pén. art. 706-95-20 II : « […] afin d'intercepter des correspondances émises ou reçues par un équipement terminal. […] »
[908] V. *supra* n°528.
[909] V. *supra* n°489.
[910] V. *supra* n°528.
[911] V. autre incohérence dans l'imbrication des écoutes téléphoniques et la captation des données : v. *supra* n°549.
[912] V. par ex. JEANDIDIER Wilfrid, *Criminalité et délinquance organisées,* Dalloz répertoire de droit pénal et de procédure pénale, al. 75 : « Ce mode de surveillance très spécifique représente un danger considérable pour les libertés, car, au lieu de cibler certains individus, il vise des zones entières […]. »

Le dispositif technique permettant la mise en œuvre est de petite taille[913] et est donc souvent installé à bord d'un véhicule. Ainsi, l'aspect mobile de ce dispositif est très intrusif. En effet, les enquêteurs utilisent, le plus souvent, cet outil associé à la filature d'un individu soupçonné, par exemple, d'un trafic de drogue. Ce sont des données qui sont collectées, non seulement tous azimuts, mais de manière itinérante, ce qui a pour effet de démultiplier la violation de la vie privée d'un nombre important de personnes non concernées par la procédure judiciaire à l'origine de l'utilisation du dispositif.

563. Le risque pour les libertés individuelles pris en compte par la loi du 23 mars 2019[914]. – Les dispositions relatives aux IMSI-catcher introduites dans la procédure pénale en 2016[915], offraient aux autorités judiciaires une complète latitude dans l'utilisation de l'IMSI-catcher. En effet, les anciens articles 706-95-4 et suivants du Code de procédure pénale alignaient le régime de l'interception de correspondances réalisée au travers de l'IMSI-catcher[916] avec celui de l'identification des terminaux mobiles[917] et de leur géolocalisation[918]. La loi du 23 mars 2019 a restreint cette utilisation de l'interception de correspondances sur deux points, rendant ainsi sensiblement plus protectrice cette investigation numérique.

564. Tout d'abord, le législateur a apporté une restriction importante à cette interception de correspondances. En effet, l'article 706-95-20 issu de la loi de mars 2019 dispose que « les correspondances interceptées […] ne peuvent concerner que la personne ou la liaison visée par l'autorisation d'interception ». Auparavant, toutes les conversations détournées par l'IMSI-catcher pouvaient être interceptées. En outre, l'interception de correspondances ne peut être mise en œuvre que pour une durée de quarante-huit heures, renouvelable[919].

565. Ensuite, une deuxième restriction découle de la censure du Conseil constitutionnel[920]. En effet, la procédure d'urgence prévue au sein des dispositions communes[921] prévoyait que les techniques spéciales d'enquêtes pouvaient, « en cas de

[913] Les autorités judiciaires parlent de « valise ».
[914] *Op. cit.* p.35
[915] V. *supra* n°555.
[916] C. pr. pén. ancien art.706-95-4 II et ancien art. 706-95-5, II. – V. *supra* n°560.
[917] V. *supra* n°558.
[918] V. *supra* n°559.
[919] V. *supra* n°556.
[920] Conseil constitutionnel, décision n°2019-778 DC du 21 mars 2019.
[921] C. pr. pén. art. 706-95-15.

risque imminent de dépérissement des preuves[922] » être mises en œuvre selon un formalisme dérogeant aux autorisations nécessaires[923] , aussi bien en enquête qu'au stade de l'information judiciaire. Le Conseil constitutionnel a censuré cette possibilité pour les enquêtes[924]. Dès lors, les IMSI-catcher ne bénéficient plus, désormais, d'une procédure d'urgence applicable en enquête. Auparavant, une telle procédure existait, non seulement pour l'identification des appareils mais également pour les interceptions de correspondances[925].

566. Un contrôle insuffisant. – Malgré les améliorations apportées par la loi du 23 mars 2019 quant à un meilleur respect des libertés individuelles, l'utilisation des IMSI-catcher demeure un acte de surveillance particulièrement intrusif. Même si la loi limite désormais l'interception de correspondances à des personnes désignées dans l'autorisation, l'accès aux données échangées par toutes les autres personnes dont les lignes ont été détournées par l'IMSI-catcher, reste possible pour les enquêteurs manipulant l'appareil. Comme souvent avec les investigations numériques, le risque d'une utilisation officieuse des informations ainsi obtenues est réel[926].

567. Dans ce contexte, l'exécution de cet acte doit faire l'objet d'un contrôle fort de la part d'un juge du siège. Or, les procédures prévues pour l'enquête policière et pour l'information judiciaire sont pratiquement identiques hormis la durée de mise en œuvre[927]. En enquête, c'est bien évidemment au juge des libertés et de la détention que sont confiées les prérogatives du juge d'instruction[928]. Dans le cas de l'enquête, c'est donc au juge des libertés qu'incombe la responsabilité du contrôle de l'exécution de la mesure[929]. Or, les positions de la doctrine et des praticiens du droit se rejoignent pour dire que les contrôles exercés par le juge d'instruction et le juge des libertés et de la détention sont totalement différents. La doctrine pénaliste parle des « limitations du contrôle du JLD », tant d'un point de vue technique puisqu'il n'est pas à l'origine de la mesure et qu'il va donc éprouver les plus grandes difficultés à apprécier l'opportunité de celle-ci,

---

[922] *Ibid.*
[923] C. pr. pén. art.706-95-12.
[924] V. *supra* n°390.
[925] C. pr. pén. ancien art.706-95-4 III.
[926] V. *supra* n°456. V. eg. LECHENET Alexandre, *Sans les nouvelles technologies, ces enquêtes journalistiques n'auraient probablement pas abouti*, Ecrans, 13 oct. 2013 : « En parcourant plusieurs quartiers d'Oslo, ils ont pu déterminer que des Imsi-catcher étaient utilisés aux alentours du quartier des ambassades et des centres de pouvoir. »
[927] V. *supra* n°556.
[928] V. C. pr. pén. art. 706-95-12
[929] C. pr. pén. art. 706-95-14.

que d'un point de vue pratique avec une accumulation conséquente de ses fonctions sans l'octroi de moyens humains supplémentaires[930]. La conséquence est évidemment un contrôle très limité, quasi « administratif », qualifié par certains auteurs « d'inconfortable[931] ». Cette situation est confirmée par les praticiens du droit qui complètent en expliquant que, par le biais du tableau de roulement des permanences des magistrats, il est très peu probable que ce soit le même juge des libertés qui contrôle l'exécution de la mesure de celui qui l'a initialement ordonné[932].

568. Conclusion du sous-paragraphe A : les IMSI-catcher. – La mise en œuvre des IMSI-catcher est le prolongement naturel de l'interception de correspondances puisqu'elle permet de contourner l'utilisation de cartes prépayées par les délinquants ou les criminels. C'est une mesure particulièrement intrusive qui dépasse la simple surveillance puisque, de manière identique à l'interception de correspondances, elle conduit à collecter un nombre important de données qu'il faut analyser. Ce besoin d'analyser des informations numériques est accrue par rapport aux écoutes téléphoniques car, avec la collecte des numéros d'IMSI, c'est un volume plus important de données qui doivent être exploitées par les enquêteurs afin d'identifier les propriétaires des lignes téléphoniques correspondantes.

569. La mise en œuvre des IMSI-catcher n'est pas le seul acte qui prolonge les effets des écoutes téléphoniques.

B. <u>La captation des données.</u>

570. Une interception de données indépendante de la ligne téléphonique. – Les écoutes téléphoniques permettent désormais d'intercepter les données qui transitent au travers de la ligne mise sous surveillance[933]. La captation des données informatiques[934]

---

[930] PELTIER Virginie, *Les écoutes judiciaires en procédure pénale : « Les preuves obtenues par IMSI-catchers et les droits fondamentaux »*, Les colloques de l'ISCJ n°2, octobre 2017.

[931] BERGERE Anne-Laure, *Le juge des libertés et de la détention, entre indépendance statutaire et dépendances matérielles*, Dalloz AJ Pénal 2019 p.120 : « […] la fonction de juge des libertés et de la détention demeure souvent jugée comme peu attractive, inconfortable tant sur le plan intellectuel que sur le plan pratique. En effet, à la diversité du champ d'intervention pouvant parfois nuire à la lisibilité de la fonction s'ajoute une mission de contrôle malaisée à cerner tant dans ses conditions d'exercice que dans son contenu. En outre, le magistrat « Jamais Là pour Dîner » est confronté à un quotidien imprévisible, souvent tardif, avec une prise de décision solitaire dans des délais très courts. »

[932] ROUCOU Denis (premier vice-président en charge du service pénal au TGI de Bordeaux), *Les écoutes judiciaires en procédure pénale : « Les problèmes juridiques posés par les nouveaux modes d'écoutes, le point de vue des magistrats »,* Les colloques de l'ISCJ n°2, octobre 2017.

[933] V. *supra* n°528.

[934] C. pr. pén. art. 706-102-1 et s.

est une investigation numérique, créée en 2011[935], qui prolonge les écoutes téléphoniques, en étendant l'interception à des données qui n'entrent pas dans le cadre de correspondances échangées par le biais d'une ligne téléphonique[936].

571. Les conditions de mise en œuvre de cette investigation numérique *(1)* sont étudiées avant ses effets *(2)*.

1. Les conditions de mise en œuvre de la captation des données

572. Des dispositions communes déjà décrites. – Tout comme les IMSI-catcher, la captation des données informatiques fait partie des techniques spéciales d'enquête, réservées aux procédures applicables à la criminalité et la délinquance organisées. L'essentiel des conditions de mise en œuvre de cet acte sont présentes dans les dispositions communes à ces techniques spéciales d'enquête[937].

573. Néanmoins, la captation des données possède des particularités qui doivent être précisées, d'une part au niveau de la cible de l'investigation *(a)* et, d'autre part, relatives au dispositif technique nécessaire pour l'exécution de l'acte *(b)*.

a. La cible de la captation des données

574. La nécessité d'une description précise de la cible de la mesure. – La décision autorisant la mise en œuvre de la captation des données[938] doit notamment préciser « la localisation exacte ou la description détaillée des systèmes de traitement automatisé de données[939] ». Ce sont donc deux éléments cumulatifs qui doivent être décrits dans l'autorisation.

575. Un système de traitement automatisé de données pour cible. – En premier lieu, la captation des données doit cibler un « système de traitement automatisé de données » (ci-après STAD). Cette notion a été introduite par la loi du 5 janvier 1988 dite « loi Godfrain[940] », lors de la création des articles 323-1 et suivants du Code pénal[941]. Malgré la définition posée par les travaux préparatoires de cette loi indiquant que, pour être un

[935] Loi n°2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure.
[936] La notion de « ligne » est utilisée à plusieurs reprises dans les dispositions relatives à l'interception de correspondances : C. pr. pén. art 100 et art. 100-7.
[937] Sur les dispositions communes aux techniques spéciales d'enquête, v. *supra* n°556.
[938] C. pr. pén. art. 706-102-1.
[939] C. pr. pén. art. 706-102-5.
[940] Loi n°88-19 du 5 janvier 1988 relative à la fraude informatique.
[941] Chapitre III : Des atteintes aux systèmes de traitement automatisé de données.

STAD, la présence d'un dispositif de sécurité est nécessaire[942], la jurisprudence a adopté une position beaucoup plus extensive de cette notion, en ne retenant pas la nécessité d'une protection pour le STAD[943]. Ainsi, la cible de la captation des données peut être n'importe quel équipement numérique : ordinateur, téléphone, tablette, serveur, etc. Dans les faits, la véritable limitation aux équipements susceptibles d'être visés par la mesure, est technique[944].

576. La description d'un lieu ou d'un système. – En second lieu, le texte dispose que le lieu où le STAD lui-même soit précisément[945] décrit dans la décision ordonnant l'acte de captation. Néanmoins, l'emploi du mot « ou » offre une importante latitude. En effet, si l'autorisation opte pour la description du lieu, cela signifie que, lorsque la mesure sera ultérieurement exécutée, le dispositif pourra être installé dans tous les équipements numériques présents au sein de ce lieu. Or, dans le cas, par exemple, d'une maison ou d'un local professionnel, il y a souvent plusieurs ordinateurs. Rien n'empêche alors que le dispositif de captation soit installé sur chacun d'eux.

b. Les autorisations relatives au dispositif technique de captation des données

577. La nécessité d'une autorisation pour la mise en place du dispositif technique. – Une telle autorisation[946], distincte de celle permettant l'acte proprement-dit de captation de données, a déjà été commenté pour la géolocalisation, notamment en raison de la complexité qu'elle crée dans les conditions de mise en œuvre de l'acte[947].

578. Les deux autorisations relatives au dispositif technique. – Dans le cadre de la captation des données, cette complexité s'accentue puisqu'il existe deux autorisations qui concernent la mise en place du dispositif technique. En premier lieu, une autorisation pour

---

[942] ROBACZEWSKI Corinne, *atteinte aux systèmes de traitement automatisé de données*, JurisClasseur Pénal Code art. 432-9, Fasc. 20 : « Pour le Sénat, la condition préalable comportait donc deux caractéristiques : d'une part, il s'agissait d'un ensemble composé d'éléments de nature diverse (unités de traitement, mémoires, logiciels, données, organes d'entrées et sorties, liaisons) dont les relations entre eux pouvaient résulter de la recherche d'un résultat déterminé (le traitement de données) ; d'autre part, il s'agissait d'un ensemble protégé par des dispositifs de sécurité. »

[943] CA Paris, 5 avr. 1994 : LPA 1995, n° 80, chron. Droit de la communication, note V. Alvarez ; JCP E 1995, I, 461, obs. F. Vivant et C. Le Stanc.
Crim. 3 oct. 2007 n°07-81.045 : JurisData n°2007-040853 - VÉRON Michel, *Le maintien frauduleux dans un système* – LexisNexis, Droit pénal n° 12, Décembre 2007, comm. 158.

[944] V. *infra* n°598.

[945] L'art. 706-102-3 parle de « localisation exacte » ou de « description détaillée ».

[946] C. pr. pén. art . 706-102-5.

[947] V. *supra* n°493.

créer des dispositifs techniques spécifiques est prévue *(α)*. En second lieu, l'autorisation de mise en place du dispositif, nécessaire pour d'autres investigations numériques comme pour la géolocalisation, offre ici de larges possibilités *(β)*.

α. L'autorisation de création d'un dispositif spécifique

579. Une possibilité unique. – Les dispositions définissant la captation des données offrent une possibilité unique en matière d'investigation numérique. Elles permettent au juge de délivrer une autorisation à une « personne physique ou morale […] en vue d'effectuer les opérations techniques permettant la réalisation du dispositif technique[948] » qui sera ultérieurement mis en place pour procéder à la captation. Cette possibilité de création d'un dispositif spécifique prend parfaitement en compte les difficultés techniques qui entourent cette mesure lorsqu'elle est exécutée[949]. L'idée semble, en effet, d'autoriser le juge à pouvoir solliciter des spécialistes de la cybersécurité pour créer ce dispositif technique spécifique. Pour autant, le texte tel qu'il est formulé soulève plusieurs commentaires.

580. L'importante limitation de l'inscription sur une liste d'experts judiciaires. – En premier lieu, l'autorisation pour créer ce dispositif technique fait référence à deux qualités cumulatives que doit posséder la personne désignée par le juge. Celle-ci doit être, à la fois, habilitée[950] et être inscrite sur une liste d'experts judiciaires[951]. La notion d'habilitation est particulièrement floue car elle ne se réfère à aucune liste ou précision qui serait apportée par voie règlementaire, comme c'est l'usage avec ce type de disposition[952]. Par ailleurs, le fait d'avoir circonscrit les personnes susceptibles d'être désignées par le juge pour créer le dispositif technique, à celles dument inscrites sur une liste d'experts judiciaires limite considérablement la portée de cette disposition, puisqu'il n'est pas évident que les spécialistes aptes à répondre à de tels besoins soient inscrits en tant qu'experts.

[948] C. pr. pén. art. 706-102-1 2ème al.
[949] V. *infra* n°598.
[950] C. pr. pén. art. 706-102-1 : « toute personne physique ou morale habilitée […]. »
[951] *Ibid.* : « […] et inscrite sur l'une des listes prévues à l'article 157 […] »
Sur les listes d'experts judiciaires, v. *supra* n°301.
[952] V. par. ex. C. pr. pén. art. 706-95-17 : « […] agent qualifié d'un service, d'une unité ou d'un organisme […] dont la liste est fixée par décret. »

581. La possibilité de saisir les services de renseignement. – En second lieu, la captation des données offre une autre possibilité pour la création du dispositif technique. Le juge peut « prescrire le recours aux moyens de l'Etat[953] », selon les mêmes modalités que pour le déchiffrement des données[954]. Il s'agit ici de pouvoir utiliser les moyens des services de renseignement. Il convient toutefois de rappeler que les moyens de l'Etat ne peuvent être sollicités que pour des infractions dont « la peine encourue est égale ou supérieure à deux ans d'emprisonnement[955] ».

582. Quoi qu'il en soit, que les autorités judiciaires choisissent de solliciter un expert judiciaire ou les services de renseignement, il se dégage une certaine logique des dispositions encadrant la captation des données. En effet, lorsque, le cas échéant, une autorisation a été délivrée pour créer un dispositif technique spécifique, et que celui-ci a été réalisé, le juge doit alors délivrer une autorisation pour installer ce dispositif.

β. Un large périmètre offert par l'autorisation d'installation du dispositif

583. Les personnes habilitées à installer le dispositif. – Les dispositions communes à toutes les techniques spéciales d'enquête prévoient que seul « un agent qualifié d'un service, d'une unité ou d'un organisme placé sous l'autorité ou la tutelle du ministre de l'intérieur ou du ministre de la défense » peut être requis pour procéder à l'installation et le retrait du dispositif technique nécessaire aux opérations de captation[956]. Par suite, outre son habilitation, cet agent doit être explicitement autorisé à installer le dispositif.

584. L'autorisation pour la mise en place du dispositif technique. – Cette autorisation, commune à d'autres investigations numériques[957], présente certaines spécificités dans le cas de la captation des données. Il ressort des dispositions relatives à l'autorisation de mise en place du dispositif technique, un doute sur le caractère facultatif de cette autorisation. En effet, le texte emploie la formule « en vue de mettre en place », et dispose que le juge peut autoriser, ce qui sous-entend qu'il n'est pas systématiquement obligé de le faire pour que la mesure puisse être exécutée. Dans les faits, cette autorisation est tout le temps nécessaire car la mise en place du dispositif technique indispensable aux

[953] C. pr. pén. art. 706-102-1 : « Le procureur de la République ou le juge d'instruction peut également prescrire le recours aux moyens de l'Etat soumis au secret de la défense nationale selon les formes prévues au chapitre Ier du titre IV du livre Ier. »
[954] V. *supra* n°408.
[955] C. pr. pén. art. 230-1 – V. *supra* n°411.
[956] C. pr. pén. art. 706-95-17.
[957] V. *supra* n°577.

opérations de captation des données, ne peut être réalisée qu'après avoir pénétré dans un lieu physique ou après l'avoir installé à distance.

585. L'autorisation de pénétration dans un lieu physique. – Le premier alinéa de l'article 706-102-5 autorise l'introduction dans un lieu physique, selon les mêmes distinctions et la même complexité qui en découle, que pour la géolocalisation[958].

586. L'autorisation de transmission par un réseau de communications électronique. – Le deuxième alinéa de ce même article mérite l'attention. En effet, l'installation du dispositif technique fait partie intégrante de l'acte de captation des données. Lorsque cette installation sera exécutée, en application de l'autorisation précédemment donnée, elle aura pour effet de permettre, à la personne habilitée à procéder à l'installation du dispositif[959], de pirater, à distance, l'ordinateur[960], puisque ce procédé consiste, au travers d'internet, à installer un code malveillant[961] sur cet ordinateur.
Ce piratage est au cœur de la captation des données lorsque la mesure entre dans ses effets.

2. Les effets de la captation des données

587. Un acte de procédure utilisant des virus informatiques. – Le dispositif technique permettant la mise en œuvre de la captation des données est un logiciel espion. Informatiquement, il fait nécessairement partie de la famille des codes malveillants. Cette situation est peu banale car il est plus fréquent que des outils soient détournés de leur utilisation légale pour commettre des infractions, que l'inverse.

588. Le lien avec les codes malveillants est explicité par le Code pénal, qui réprime « la fabrication, l'importation, la détention, l'exposition, l'offre, la location, la vente et la publicité » de tels dispositifs[962]. L'article 226-3 fait référence à la captation des

[958] V. *supra* n°493.
[959] V. *supra* n°583.
[960] Ou tout autre équipement informatique, v. *supra* n°575.
[961] V. *infra* n°587.
[962] C. pén. art. 226-3. Ce sont, notamment, les outils permettant les écoutes téléphoniques et les captations de données, réalisées de manière illégale qui sont visés par cet article.

données[963]. L'illustration n°2 (en page suivante) met en relation des familles de virus informatiques avec les dispositions de la captation des données.

Extrait de l'art. 706-102-1	Code malveillant correspondant
« telles qu'elles s'affichent sur un écran pour un utilisateur »	*Screen logger* qui capte tout ce qui s'affiche sur un écran
« telles qu'il les y introduit par saisie de caractères »	*Keylogger* qui capte les caractères saisis par un clavier ou un autre périphérique d'entrée
« telles qu'elles sont stockées dans un système informatique »	Cheval de troie, *backdoor server*

Illustration n°2 : tableau présentant les codes malveillants permettant d'accomplir la mesure

589. Un acte considérablement étendu par la loi de 2016. – La loi du 3 juin 2016[964], particulièrement sécuritaire dans le contexte de risque terroriste[965], a modifié la captation des données, en étendant considérablement les possibilités d'investigation. En effet, la loi de juin 2016 a ajouté la dernière ligne au tableau de l'illustration n°2, ce qui a complétement modifié les effets de la captation des données.

590. Antérieurement à la loi de juin 2016, seules certaines données pouvaient être interceptées et, en aucun cas, la captation des données informatiques ne devait se transformer en perquisition informatique[966]. La doctrine expliquait que « cette captation de données avait pour effet de mettre l'enquêteur dans la situation de quelqu'un qui observerait derrière lui l'utilisateur d'un ordinateur[967] ». Ainsi, la mise en place d'un dispositif de captation, ne devait pas permettre d'avoir accès aux données qui étaient déjà stockées dans le terminal faisant l'objet de la mesure[968].

[963] *Ibid*. « […] permettent de réaliser l'infraction prévue par l'article 226-1 ou ayant pour objet la captation de données informatiques prévue aux articles 706-102-1 du code de procédure pénale […] ».
[964] Loi n°2016-731 du 3 juin 2016 (*op. cit.* p.23).
[965] RIBEYRE Cédric, *Loi n°2016-731 du 3 juin 2016 [...] – Et maintenant ?* Droit pénal LexisNexis n°9, septembre 2016, étude 17.
[966] La perquisition de données ou de systèmes informatiques existe et est prévue par d'autres dispositions du Code de procédure pénale : v. *supra* n°250. et s.
[967] *Op. cit.* p.31 PRADEL Jean, *Procédure pénale*, p. 455.
[968] Typiquement, cela signifiait que l'enquêteur ne devait pas fouiller les données enregistrées dans le disque dur ou sur un support de stockage amovible (clé USB, disque externe) si ces données n'étaient pas affichées à l'écran par l'utilisateur de l'ordinateur.

591. Un acte très proche de la perquisition dans ses effets. – La loi de 2016 a introduit la possibilité de pouvoir accéder à des données « telles qu'elles sont stockées dans un système informatique », ce qui ouvre un vaste périmètre, au point qu'il est nécessaire de s'interroger s'il ne s'agit pas désormais d'une perquisition. Cette question fait partie des ambiguïtés qui entourent les régimes des investigations numériques, car elle se pose pour plusieurs actes. Dans le cas de la captation des données, le raisonnement est identique à celui développé pour la fouille des messageries numériques[969].

592. La doctrine n'est pas unanime sur les notions de lieu clos, caractéristique essentielle de la perquisition, et de domicile virtuel qui pourrait constituer le prérequis nécessaire à la définition de l'acte de perquisition[970]. En revanche, les auteurs s'accordent sur le caractère particulièrement attentatoire aux libertés individuelles des investigations numériques comme la captation des données ou la fouille des messageries électroniques qui sont très proches de la perquisition dans leurs effets, mais bénéficiant d'un régime considérablement plus souple.

593. En premier lieu, la captation des données peut être mise en œuvre pour des durées très longues par rapport à une perquisition, à savoir d'au moins un mois[971]. En second lieu, alors que la perquisition est systématiquement portée à la connaissance des personnes concernées, la captation des données se déroule totalement à l'insu des personnes surveillées[972].

594. La difficulté de contrôler les informations réellement obtenues. – La question d'une utilisation détournée ou, à tout le moins, non officielle, des données auxquelles les enquêteurs ont réellement accès concerne beaucoup d'investigations numériques. Comme précédemment expliqué pour la sonorisation et la fixation d'images[973] ou pour les IMSI-

---

[969] V. *supra* n°366.
[970] *Op. cit.* p.35.
[970] DECIMA Olivier, *Du piratage informatique aux perquisitions et saisies numériques ?* Dalloz AJ pénal 2017.
SAINT-PAU Jean-Christophe, *Les investigations numériques et le droit au respect de la vie privée,* Dalloz AJ pénal 2017.
DUMENIL Gabriel, *Vers une dématérialisation du domicile : réflexions autour de la théorie du domicile virtuel en droit pénal,* LexisNexis, Droit pénal n° 7-8, Juillet 2019, étude n°17.
DESPORTES Frédéric et LAZERGES-COUSQUER Laurence, *Traité de procédure pénale,* Economica.
[971] C. pr. pén. art. 706-95-16 : jusqu'à un mois en enquête et jusqu'à deux ans à l'instruction.
[972] Sur l'absence totale d'information, v. *supra* n°368.
[973] V. *supra* n°457.

catcher[974], les enquêteurs peuvent, au travers du dispositif utilisé, avoir accès à des informations sans que celles-ci ne soient actées dans la procédure. La captation des données est l'investigation numérique qui ouvre des possibilités de détournements très importantes. En effet, l'enquêteur qui fouille les fichiers enregistrés sur l'ordinateur peut avoir accès à toutes les informations personnelles de son utilisateur[975]. Même si le texte dispose que seules « les données qui sont utiles à la manifestation de la vérité [sont retranscrites dans un procès-verbal et] qu'aucune séquence relative à la vie privée étrangère aux infractions visées dans les ordonnances autorisant la mesure ne peut être conservée dans le dossier de la procédure », les enquêteurs peuvent avoir accès à une multitude d'informations personnelles contenues dans l'ordinateur espionné, et il est impossible pour la personne ayant fait l'objet de la mesure, d'en connaître la liste exhaustive.

595. Un acte ambivalent. – Les modifications de la captation des donnés par la loi de 2016[976], ont pour conséquence de rendre cet acte ambivalent au sein de la procédure pénale. En effet, lorsqu'il a été créé en 2011[977], aucun doute n'était possible sur l'objectif de surveillance de cette mesure. L'illustration la plus évidente de cet objectif, était la description imagée de l'enquêteur qui observait virtuellement l'écran de l'individu surveillé par-dessus son épaule[978]. Depuis que la captation des données permet d'accéder aux informations telles qu'elles sont stockées dans un système informatique, elle est devenue un acte de fouille à part entière, puisqu'elle repose sur une action forte de la part de l'enquêteur[979]. En ce sens elle est différente des actes de surveillance qui permettent d'obtenir des données passivement, dès que le dispositif est mis en place, comme c'est le cas avec les écoutes téléphoniques[980].

596. Pour autant, le choix a été fait de classer la captation des données au sein des actes de surveillance dans la présente étude, en raison de l'esprit qui entourait cette mesure

[974] V. *supra* n°566.
[975] Voire de plusieurs utilisateurs s'il s'agit d'un ordinateur familial utilisé par plusieurs membres de la famille.
[976] V. *supra* n°589.
[977] V. *supra* n°570.
[978] PRADEL Jean, *Procédure pénale*, v. *supra* n°589.
[979] L'accès aux données stockées dans le système informatique suppose des actions de la part des enquêteurs, à la différence d'un *keylogger* ou d'un *screen logger* (voir illustration n°2) qui collecte passivement des informations.
[980] V. *supra* n°538.

lorsqu'elle a été créée, même si elle trouverait maintenant sa place dans les actes de fouille de données[981].

597. Conclusion du sous-paragraphe B : la captation des donnés. – La captation des données est une investigation numérique qui permet de prolonger les écoutes téléphoniques, puisque ces deux mesures ont pour effet d'intercepter un flux d'informations numériques. Les écoutes téléphoniques autorisent uniquement l'interception du flux de données transitant au travers d'une ligne téléphonique, tandis que la captation permet d'intercepter les informations directement sur, par exemple, un ordinateur, telles qu'elles sont saisies par l'utilisateur ou telles qu'elles s'affichent à l'écran[982]. La captation de données a considérablement été étendue dans ses effets en 2016, lui conférant maintenant les caractéristiques d'un acte de fouille, puisque cette mesure offre la possibilité aux enquêteurs d'accéder aux informations enregistrées dans le terminal numérique ciblé. En conséquence, la captation des données fournit une puissance d'investigation considérable aux autorités judiciaires puisque, d'une part, elle peut cibler n'importe quel objet numérique[983] et que, d'autre part, elle autorise la fouille des données enregistrées dans cet objet numérique.

598. En fait, les réelles limitations sont techniques, car cette investigation numérique est d'une grande complexité dans sa phase d'exécution. Elle suppose des compétences de hauts niveaux, surtout si le dispositif est installé à distance[984]. Le législateur a pris conscience de cette difficulté puisque les dispositions encadrant la captation des données prévoient que des spécialistes de la cybersécurité ou les services de renseignements peuvent être sollicités pour créer le dispositif technique permettant de mettre en œuvre la réalisation de la mesure.

599. Conclusion du paragraphe §2 : les actes dépassant la simple surveillance. – Les investigations numériques pour la surveillance d'individus, comportent parfois des actions qui dépassent le simple espionnage. C'est le cas avec les écoutes téléphoniques et les actes ont été créés pour prolonger les effets de celles-ci[985], qui ont en commun

[981] V. *supra* n°243.
[982] V. *supra* n°590.
[983] L'art 706-102-1 du C. pr. pén. renvoi à la notion de « systèmes de traitement automatisé de données », qui est entendue de manière très extensive par la jurisprudence : v. *supra* n°575.
[984] V. *supra* n°586.
[985] Les IMSI-catcher (v. *supra* n°553.) et la captation des données (v. *supra* n°570.).

d'intercepter un flux de données. Les informations numériques ainsi obtenues peuvent représenter un volume important, qu'il n'est pas possible d'exploiter en direct. Ainsi, ces mesures prévoient implicitement que les données obtenues puissent être analysées lors de l'exécution de l'acte lui-même.

600. Conclusion de la section 2 : l'obtention de données par des actes de surveillance. – Les investigations numériques destinées à la surveillance d'individus sont éparpillées dans le Code de procédure pénale. Elles font partie, aussi bien de la procédure de droit commun dans le cas, notamment, de la géolocalisation[986] ou des écoutes téléphoniques[987], que de la procédure dérogatoire prévue pour la criminalité et la délinquance organisées, comme avec les IMSI-catcher[988] et la captation des données[989]. De plus, cet éparpillement est instable puisque l'enquête sous pseudonyme[990] a été déplacée récemment[991] depuis les actes prévus au sein de la procédure dérogatoire vers la procédure de droit commun. Cette modification s'accompagne évidemment d'un changement de régime. Or, les investigations numériques de surveillance, tout comme celles prévues pour la fouille des données[992], reposent sur une multitude de régimes différents. Ce sont tout particulièrement les régimes entourant les autorisations nécessaires à la mise en place du dispositif permettant l'exécution de la mesure qui diffèrent d'un acte à l'autre. Ces autorisations de mise en place sont distinctes de l'autorisation de l'acte lui-même, ce qui complexifie leurs régimes, déjà compliqués en raison des rôles dévolus au juge d'instruction, au procureur de la république et au juge des libertés et de la détention. En effet, selon que l'acte est ordonné en enquête, au stade de l'information judiciaire, ou en procédure d'urgence, l'intervention de ces magistrats s'entrecroise ou se chevauche.

601. Conclusion du chapitre 1 : les régimes de l'obtention de données par des actes intrusifs. – Les investigations numériques en procédure pénale sont des actes dont les effets comportent l'obtention de données. Ces dernières peuvent être recueillies lors

[986] V. *supra* n°489.
[987] V. *supra* n°528.
[988] V. *supra* n°553.
[989] V. *supra* n°570.
[990] V. *supra* n°468.
[991] Loi n°2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice.
[992] V. *supra* n°243.

d'actes de fouille, tel que la perquisition[993] qui comporte une véritable perquisition informatique[994] en son sein. Les données obtenues au travers des actes de fouille sont des informations numériques générées intentionnellement par la personne visée par la mesure[995]. En effet, l'individu, au travers de l'utilisation qu'il fait des outils numériques, crée des données. Les investigations numériques de fouille ont alors pour finalité de permettre aux enquêteurs d'accéder à celles-ci. Dans le cas des investigations numériques destinées à la surveillance des personnes, il existe deux cas de figure. En premier lieu, les enquêteurs peuvent espionner des données qui sont également générées par l'individu surveillé. C'est notamment le cas avec les écoutes téléphoniques : les enquêteurs espionnent les données que la personne surveillée crée en utilisant son téléphone.

En second lieu, les autorités judiciaires peuvent surveiller un individu au travers de données que celui-ci génère à son insu. Ces données n'auraient jamais existé sans la mesure de surveillance[996], comme dans le cas de la géolocalisation réalisée au travers d'un dispositif technique spécifique[997]. Qu'elles soient générées intentionnellement ou pas, les données obtenues dans le cadre des mesures de surveillance ou de fouille d'informations numériques, ont en commun d'être le fruit d'actes particulièrement intrusifs dans la vie privée des personnes ciblées par ces mesures.

602. Il existe une autre catégorie d'investigations numériques, moins intrusive, qui permet aux autorités judiciaires d'obtenir des informations. Ces dernières sont extraites des traitements de données judiciaires.

[993] V. *supra* n°244.
[994] V. *supra* n°254.
[995] V. *supra* n°57.
[996] V. *supra* n°67.
[997] V. *supra* n°501.

Chapitre 2. Les régimes de l'extraction de données depuis les traitements judiciaires

603. L'extraction d'informations depuis les traitements de données judiciaires. – La numérisation de notre société et du monde professionnel[998] a pour effet de dématérialiser les informations utilisées par les autorités judiciaires dans leur travail quotidien[999]. Cette dématérialisation se traduit, notamment, par la création d'une multitude de traitements de données à caractère personnel relatifs aux antécédents judiciaires des personnes condamnées voire, plus généralement, de toutes celles dont le nom apparaît dans les enquêtes. Or, les investigations numériques en procédure pénale sont des actes qui ont pour effet d'obtenir ou de générer des données potentiellement disponibles pour la suite de l'enquête. En conséquence, la consultation et l'extraction de données depuis les traitements de données mis en œuvre par les autorités judiciaires sont des investigations numériques à part entière[1000].

604. Le caractère non intrusif de ces investigations numériques. – L'obtention de données au travers de l'interrogation des traitements judiciaires constitue une deuxième catégorie d'investigations numériques. En effet, elles diffèrent de celles permettant d'obtenir des données au travers d'actes intrusifs[1001], car elles placent l'enquêteur dans un « travail de bureau ». Au travers de cette catégorie d'investigations numériques, les autorités judiciaires obtiennent des données sans avoir, ni à se rendre sur des lieux précis, ni à convoquer et entendre un individu. Ces informations étaient déjà en possession des autorités judiciaires puisqu'elles ont été enregistrées dans le traitement lors de procédures antérieures. Cette extraction de données n'est donc pas un acte intrusif.

605. La pluralité des régimes des traitements judiciaires. – Les traitements judiciaires sont éparpillés dans le Code de procédure pénale ainsi que dans une multitude de textes. Il en résulte une pluralité des régimes encadrant leurs conditions de mise en œuvre, l'enregistrement des informations, leur contrôle et, bien sûr, leur consultation

[998] Sur l'influence de la numérisation sur les activités professionnelles, v. *supra* n°21.
[999] V. *supra* n°72.
[1000] V. *supra* n°155.
[1001] V. *supra* n°235.

conduisant à l'extraction de données. Ainsi, tout comme pour les actes intrusifs, il n'existe pas d'autres moyens que de procéder à l'étude de ces traitements de données afin d'en déterminer les régimes permettant d'en extraire des informations.

606. Pour autant, il existe un nombre très important de traitements de données utilisés par les autorités judiciaires. Il est donc nécessaire, préalablement, de définir les critères qui font que leur consultation constitue une investigation numérique *(Section 1)*, avant de pouvoir étudier les régimes des traitements répondant à ces conditions *(Section 2)*.

Section 1. La nécessité de clarifier le foisonnement des traitements judiciaires

607. La nécessité de faire progresser l'enquête. – L'influence de la numérisation de notre société sur les environnements professionnels s'est traduite par la création d'une multitude de traitements de données utilisés par les autorités judiciaires. Néanmoins, la consultation de ces traitements ne constitue pas toujours une investigation numérique. En effet, ils n'ont pas tous vocation à fournir des preuves[1002]. Certains ont une finalité de gestion administrative des dossiers[1003].

608. Ainsi, il est nécessaire de clarifier ce contexte global de foisonnement des traitements *(§1)*, pour être en mesure de distinguer efficacement les traitements dont la consultation est susceptible de constituer une investigation numérique, de ceux qui doivent être écartés au motif qu'ils n'ont pas vocation à fournir des éléments de preuve et donc à faire progresser l'enquête *(§2)*.

§1. Le contexte général entourant les traitements judiciaires

609. La notion de traitements de données à caractère personnel. – Celle-ci est définie par le règlement général sur la protection des données (RGPD)[1004]. Dans la suite

[1002] Sur la notion de preuve : v. *supra* n°179.
[1003] V. *supra* n°52.
[1004] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).
Article 4 : « […]
1) «données à caractère personnel», toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée «personne concernée»); est réputée être une «personne physique identifiable» une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un

des présentes, l'appellation « traitement judiciaire » désigne tout traitement de données à caractère personnel directement accessible aux autorités judiciaires au stade de l'enquête[1005]. Cette appellation est considérée comme synonyme des notions informatiques de « fichier » ou de « base de données ». Ces termes sont donc utilisés indifféremment dans la présente étude.

610. La distinction de l'accès aux informations enregistrées dans des traitements de données par la réquisition. – Il est souvent essentiel pour l'efficacité de l'enquête, que les autorités judiciaires puissent avoir accès à des informations enregistrées dans un traitement de données. Lorsque ce dernier est mis en œuvre par des tiers[1006], les données sont obtenues par le biais d'une réquisition[1007].

611. De nombreux traitements. – Il existe un nombre très important de traitements de données mis en œuvre par l'Etat pour son fonctionnement. Ceux-ci dépassent nettement le cadre des fichiers judiciaires, et ont de vastes finalités[1008]. Ils sont souvent utiles aux citoyens pour, par exemple, percevoir des prestations, pour s'acquitter simplement des factures de cantine scolaire ou pour recevoir un repas à domicile[1009]. Bien que mis en œuvre par l'Etat, ses administrations ou des collectivités territoriales, les enquêteurs doivent utiliser une réquisition pour obtenir les données enregistrées dans ces traitements.

612. Le critère de l'accès direct aux informations. – L'extraction des données depuis les traitements judiciaires dont il est question ici, se distingue par le fait qu'un accès direct est prévu, par un texte, pour les autorités judiciaires au stade de l'enquête. Cet accès direct offre deux avantages. Tout d'abord, les enquêteurs accèdent beaucoup plus rapidement

---

identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale;
2) «traitement», 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;
[…] »

[1005] Crim. 15 septembre 2009 n°09-82.597 Bull. crim. 2009, n° 155. Recueil Dalloz 2009 p.2428, *La consultation des fichiers de police ne nécessite pas de réquisition.*

[1006] Entreprise privée comme un opérateur de téléphonique, établissement public comme un organisme délivrant des prestations sociales, etc.

[1007] Sur l'obtention de données auprès de tiers, v. *supra* n°372.

[1008] Suivi administratif des personnes faisant l'objet de soins psychiatriques sans consentement (Décret n°2018-383 du 23 mai 2018), sécurité sociale, prestations sociales, Schengen, suivi scolaire des enfants, etc.

[1009] Dans le cadre du maintien à domicile : prestation réalisée par les Conseils départementaux.

aux informations que lorsqu'ils doivent utiliser une réquisition. Ensuite, l'accès direct offre une confidentialité totale vis-à-vis de la personne ciblée par la recherche d'informations. Cette confidentialité n'est effectivement pas garantie lorsque les autorités judiciaires requièrent un tiers pour obtenir des données. En effet, dans certaines situations, rien n'empêche qu'un salarié ou un agent travaillant chez ce tiers informe l'individu ciblé par la réquisition, que la justice s'intéresse à lui.

613. Le dépassement des traitements judiciaires. – Il existe de nombreux traitements de données à caractère personnel mis en œuvre par l'Etat pour lesquels un accès est directement prévu lors d'une enquête pénale sans que, pour autant, ces traitements soient mis en œuvre par les autorités judiciaires. Il en est ainsi de fichiers administratifs comme, par exemple, le fichier national des immatriculations[1010], ou de certains traitements propres à l'activité de renseignement. Ces derniers sont inconnus du public, car ils sont couverts par le secret défense[1011], en bénéficiant du régime dérogatoire prévu par la loi informatique et libertés[1012]. Plusieurs de ces fichiers ont un accès directement ouvert aux enquêteurs et sont donc étudiés dans la suite des présentes.

614. En conséquence, il convient de rappeler que l'appellation « traitement judiciaire » telle qu'utilisée dans la présente étude signifie « tout traitement de données à caractère personnel pour lequel un accès est directement prévu en enquête pénale », peu importe qu'il soit mis en œuvre par les autorités judiciaires ou par un autre service de l'Etat.

615. L'impossibilité de recenser les traitements judiciaires. – En premier lieu, aussi surprenant que cela puisse paraître, il existe un nombre indéterminé de « fichiers de police et de gendarmerie[1013] ». En 2010, les « directions générales de la Police et de la

[1010] V. *infra* n°698.

[1011] V. par ex. CRISTINA (centralisation du renseignement intérieur pour la sécurité du territoire et des intérêts nationaux) ou, en matière de terrorisme, le FSPRT dont la création a été notifiée par le décret du 2 août 2017 modifiant le décret du 5 mars 2015 portant création d'un traitement automatisé de données à caractère personnel dénommé « Fichier de traitement des signalements pour la prévention de la radicalisation à caractère terroriste » (FSPRT) », et GESTEREXT, créé par le décret n°2017-1218 du 2 août 2017 modifiant les articles R. 211-32 et R. 841-2 du code de la sécurité intérieure.

[1012] Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par l'ordonnance du 12 décembre 2018, art. 33 : « Les demandes d'avis portant sur les traitements intéressant la sûreté de l'Etat, la défense ou la sécurité publique peuvent ne pas comporter tous les éléments d'information énumérés ci-dessus. » - Art. 31 : « III.- Certains traitements […] peuvent être dispensés, par décret pris en Conseil d'état, de la publication de l'acte réglementaire qui les autorise. […] »
V. le décret n°2007-914 du 15 mai 2007 pris pour l'application du I de l'article 30 (ancienne codification) de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

[1013] BAUER Alain et SOULLEZ Christophe, *Les fichiers de police et de gendarmerie,* puf, collection Que sais-je ?

Gendarmerie ont entrepris de recenser, de manière exhaustive, l'ensemble des traitements de données à caractère personnel, qu'ils soient locaux[1014] ou centraux […][1015] ». Ainsi, le seul fait que les directions des deux entités habilitées à enquêter soient contraintes d'entreprendre une démarche destinée à identifier l'ensemble des bases de données comportant des informations collectées par les officiers de police judiciaire est hautement révélatrice du manque de rigueur qui entoure ces fichiers.

616. Porteur d'une parole officielle, le rapport BATHO/BENISTI[1016] précise avec beaucoup de prudence qu'en 2011, ce sont 80 fichiers de police qui sont recensés par la mission d'information, contre 58 en 2009[1017]. « L'augmentation du nombre de fichiers utilisés par rapport à 2009 est principalement imputable à la découverte de fichiers qui existaient déjà à cette date, mais dont l'existence n'avait pas été portée à la connaissance de la mission d'information, malgré ses demandes ». De plus, les auteurs du rapport indiquent qu'ils ont pu constater que certains offices centraux se livrent à du développement informatique sous *Windev*[1018] afin de créer leur propre base de données, voire même de procéder à du rapprochement[1019] sur les bases auxquelles ils ont accès[1020].

617. En deuxième lieu, dans un tel contexte, il est impossible de recenser exhaustivement les traitements de donnée auxquels ont véritablement accès les enquêteurs, d'autant plus que de nouveaux traitements apparaissent régulièrement, tant au niveau national[1021] qu'européen[1022].

[1014] V. *infra* n°1017.

[1015] *Ibid.* BAUER et SOULLEZ p.73.

[1016] BATHO Delphine et BENISTI Jacques-Alain, *rapport d'information sur la mise en œuvre des conclusions de la mission d'information sur les fichiers de police,* Commission des lois constitutionnelles, de la législation et de l'administration générale de la République de l'Assemblée Nationale, enregistré le 21 décembre 2011, p. 9 et p.28.

[1017] BATHO Delphine et BENISTI Jacques-Alain, *rapport d'information sur les fichiers de police,* Commission des lois constitutionnelles, de la législation et de l'administration générale de la République de l'Assemblée Nationale, enregistré le 24 mars 2009. Le rapport de 2011 fait suite à celui de 2009, notamment sur la mise en œuvre des préconisations qui avaient été réalisées.

[1018] *Windev* est un outil permettant de faire du développement, autrement formulé de créer ses propres programmes informatiques.

[1019] A l'identique de ce qui est prévu pour les logiciels de rapprochement judiciaire ou les fichiers d'analyse sérielle - V. *infra* n°720.

[1020] *Ibid.* BATHO Delphine et BENISTI Jacques-Alain, *rapport d'information sur la mise en œuvre des conclusions de la mission d'information sur les fichiers de police,* p.29.

[1021] V. par ex. le 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).
D'autres fichiers sont à l'étude ou en préparation tel « le fichier autonome de reconnaissance faciale » (*Ibid.* Rapport BATHO/BENISTI de 2011 p. 97), ou encore OCTOPUS, LUPIN, CORAIL, etc (*Ibid.* Rapport BATHO/BENISTI de 2011 p. 29).

[1022] Mise en œuvre d'un registre judiciaire antiterroriste en septembre 2019. Conseil Justice et affaires intérieures : compte-rendu de la réunion des 7 et 8 octobre 2019 (Source : www.consilium.europa.eu).

618. En troisième et dernier lieu, une autre raison fait qu'il n'est pas possible d'établir une liste complète car, « parmi les fichiers […] utilisés, [certains] n'ont fait l'objet ni d'une déclaration à la CNIL, ni d'un texte législatif ou réglementaire, soit 45 % des fichiers utilisés[1023] ».

619. Le paradoxe entre l'impossibilité de recenser les traitements et leur utilisation grandissante. – Il est d'autant plus dommageable d'être dans l'incapacité de pouvoir recenser exhaustivement les traitements judiciaires, que ceux-ci prennent désormais une importance considérable dans l'activité quotidienne des forces de l'ordre[1024].

620. A titre d'exemple, la loi du 3 juin 2016[1025] a créé une « retenue[1026] » aux fins « d'un contrôle ou d'une vérification d'identité », qui est en lien direct avec la consultation de ces traitements. En effet, l'article 78-3-1 du Code procédure pénale dispose que, lors de la vérification de la situation de la personne retenue, l'officier de police judiciaire peut consulter « les traitements automatisés de données à caractère personnel relevant de l'article 31 » de la nouvelle loi informatique et liberté. La description est suffisamment vague pour en déduire qu'en fonction des faits et du contexte du « placement en retenue » de la personne contrôlée, l'ensemble des fichiers accessibles aux policiers et aux gendarmes puisse être potentiellement consulté à cette occasion.

621. Conclusion du paragraphe §1 : le contexte général entourant les traitements judiciaires. – Dans la présente étude, l'appellation « traitement judiciaire » désigne tout traitement de données à caractère personnel pour lequel un accès direct aux informations qui y sont stockées est prévu en enquête pénale. Les traitements judiciaires ne sont pas uniquement mis en œuvre par les autorités judiciaires. Certains fichiers gérés par d'autres administrations sont, tout de même, directement accessibles par les enquêteurs. Les

---

[1023] *Ibid.* Rapport BATHO/BENISTI de 2011, p. 10.

[1024] VEDEL Renaud, *Le rôle des fichiers dans l'action opérationnelle des services de sécurité intérieure*, Dalloz AJ pénal 2007 p.64 : « Une police sans documentation par fichier serait entravée car sans mémoire, sans capacité d'investigation à un coût supportable, sans moyen de preuve. »

[1025] Loi n°2016-731 du 3 juin 2016 (*op. cit.* p.23).

[1026] Cette « retenue » n'est pas une garde à vue, mais elle en est toutefois proche dans l'esprit puisque l'art. 78-3-1 du C. pr. pén. parle de « placement en retenue », comme on parlerait de placement en garde à vue. Elle est limitée dans le temps (4H00 maximum), et réservée à un « comportement [qui] peut-être lié à des activités à caractère terroriste ».
RIBEYRE Cédric, *Loi n°2016-731 du 3 juin 2016 […] – Et maintenant ?* Droit pénal LexisNexis n°9, septembre 2016, étude 17 : « Une hypothèse de privation de liberté voit le jour à l'article 78-3-1 du même Code […]. »

traitements judiciaires ont tellement foisonné dans le contexte de numérisation de notre société qu'il est impossible de les recenser exhaustivement. Pour autant, pour que la consultation de ces fichiers soit susceptible de constituer une investigation numérique, il ne suffit pas que le traitement soit directement accessible aux enquêteurs. Il faut une condition cumulative afin d'être en mesure d'identifier les traitements judiciaires correspondants : les données extraites doivent concourir à faire progresser l'enquête.

§2. L'identification des traitements judiciaires

622. Les traitements de données à vocation de support administratif écartés. – Parmi la multitude de traitements judiciaires auxquels les enquêteurs ont accès directement pour les besoins des procédures dont ils sont saisis, tous ne sont pas susceptibles de constituer pas une investigation numérique. Comme précédemment expliqué, il convient de différencier la dématérialisation du support administratif des procédures[1027] de la dématérialisation des investigations[1028]. Or, la consultation des traitements de données, certes accessibles par les autorités judiciaires puisque concourant au bon déroulement d'un dossier pénal, mais dont la finalité n'est pas de fournir des éléments de preuve en enquête, ne constitue pas une investigation numérique. En effet, ces traitements ne contribuent pas à faire progresser une enquête comme le fait, par exemple, la consultation du fichier des empreintes digitales[1029] qui permet, potentiellement, d'identifier un individu présent sur une scène de crime.

623. Le rôle particulier de Cassiopée. – A première vue, Cassiopée [1030] entre dans cette catégorie des traitements dont la fonction est de servir de support numérique au bon déroulement des procédures. En effet, la finalité principale de Cassiopée est de rationaliser l'activité des magistrats des juridictions répressives en évitant, par exemple,

[1027] V. *supra* n°52.
[1028] V. *supra* n°53.
[1029] V. *infra* n°661.
[1030] C. pr. pén. art. 48-1 : « du bureau national automatisé des procédures judiciaires ».
C. pr. pén. art. R. 15-33-66-4 et s. : « du bureau national automatisé des procédures judiciaires et du traitement automatisé dénommé « Cassiopée » ».

que deux procédures soient ouvertes dans deux tribunaux différents pour les mêmes faits[1031], et en permettant un suivi administratif[1032] efficace d'un dossier.

624. D'ailleurs, dans le concret de l'activité d'enquête, ce n'est pas dans Cassiopée que les officiers de police judiciaire recherchent une information, même si celui-ci contient une description des faits délictueux ou criminels faisant l'objet d'une procédure. Ces mêmes données sont contenues dans d'autres fichiers qui sont présentés ci-après, beaucoup plus étoffés et accessibles aux enquêteurs au travers du système d'information dédié à leur activité. La seule information potentiellement intéressante aux enquêteurs, qui n'est pas obligatoirement présente dans d'autres fichiers de police, concerne les données bancaires enregistrées dans Cassiopée. Celles-ci pourraient s'avérer utiles au sein d'une procédure de recouvrement, dans une situation où une personne condamnée tenterait de se soustraire au paiement d'une amende ou de la somme qu'elle devrait à une partie civile.

625. Pourtant, même si la consultation de Cassiopée n'entre pas dans la catégorie des investigations numériques, celui-ci constitue un élément central au sein des fichiers de police dont la consultation est une investigation numérique. En effet, les travaux actuels visant à poursuivre la dématérialisation de la procédure pénale[1033] ont pour objectif de créer des interconnexions entre Cassiopée et, notamment, le Traitement des Antécédents Judiciaires et les logiciels de rédaction des procédures[1034] utilisés par la Police et la Gendarmerie pour tenter d'améliorer les mises à jour des données dans ces deux bases de données[1035]. Ce dernier point confirme bien le côté « administratif » de Cassiopée qui est positionné comme la base faisant foi pour la fiabilité des données pénales sur lesquelles reposent les procédures, très certainement parce que ce traitement est placé sous le

---

[1031] *Op. cit.* p.20 TOURE Aminata, *L'influence des nouvelles technologies dans l'administration de la justice pénale* : « L'objectif [de Cassiopée] est de faciliter le regroupement des procédures mettant en cause les mêmes personnes et ainsi, éviter les doubles poursuites. »

[1032] Le mot « administratif » ne doit pas être ici entendu au sens de police ou d'enquête administrative, mais au sens d'administration d'un dossier.

[1033] V. *supra* n°50.

[1034] Pour le traitement d'antécédents judiciaires : v. *infra* n°642. Pour le LRPGN pour la Gendarmerie et le LRPPN pour la Police : v. *infra* n°.649. V. circulaire du 18 août 2014 relative aux fichiers d'antécédents judiciaires (Bulletin officiel du Ministère de la justice), p.6 : « Les échanges inter-applicatifs entre CASSIOPEE et le TAJ ».
V. également, *op. cit.* p.20 SONTAG KOENIG Sophie, *Technologies de l'information et de la communication et défense pénale*. P. 247 et 248.

[1035] CNIL, délibération n°2011-233 du 21 juillet 2011 portant avis sur un projet de décret en Conseil d'Etat renforçant l'efficacité et la sécurité du bureau d'ordre national automatisé des procédures judiciaires dénommé « Cassiopée ».
CNIL, délibération n° 2011-420 du 15 décembre 2011 portant avis sur un complément au projet de décret en Conseil d'Etat renforçant l'efficacité et la sécurité du bureau d'ordre national automatisé des procédures judiciaires dénommé « Cassiopée ».

contrôle des magistrats. Néanmoins, au travers de ce rôle de base de référence pour les autres fichiers de police, Cassiopée tend à jouer un rôle crucial dans l'avenir[1036].

626. Des fichiers de police écartés en raison d'un périmètre trop restreint. – Certains traitements de données, dont la consultation est susceptible de constituer une investigation numérique car ils contiennent potentiellement des éléments de preuve, sont écartés de la présente étude, au motif qu'ils concernent un périmètre géographique limité à la Préfecture de Paris. C'est le cas d'Octopus qui a pour finalité de collecter les signatures graphiques des *taggeurs* afin de pouvoir réprimer plus efficacement les infractions correspondantes[1037]. On pourrait imaginer qu'un *taggeur* soit impliqué dans des faits beaucoup plus graves (ou qu'il soit un témoin clé d'un crime ou d'un délit) et que les informations contenues dans cette base de données soient susceptibles de faire avancer une enquête. Toutefois, la limitation géographique à la Préfecture de Paris amoindrit considérablement son intérêt dans une étude à la portée générale. La situation est similaire avec GEVI[1038], dont le périmètre est également limité à la Préfecture de Police de Paris.

627. Des fichiers liés à la détention écartés. – Plusieurs traitements de données liés à la détention et au monde carcéral contiennent des informations sur le passé judiciaire d'individus. Ceux-ci ne sont pas, non plus, étudiés ici car ils ne présentent pas d'intérêt en tant qu'investigation numérique. Soit les informations qu'ils contiennent sont déjà présentent dans d'autres fichiers plus facilement accessibles aux enquêteurs[1039], soit ce sont des données liées à l'exécution de la peine prononcée à l'encontre d'un individu[1040].

628. Conclusion de la section 1 : la nécessité de clarifier le foisonnement des traitements judiciaires. – Il existe une multitude de traitements de données à caractère personnel contenant des informations nécessaires au bon fonctionnement des procédures pénales. Certains de ces fichiers ont une vocation administrative dans le sens où ils

[1036] V. *infra* n°1172.
[1037] C. pén art. 322-1 et R635-1.
[1038] Gestion des violences urbaines.
[1039] Par exemple, le traitement d'antécédents judiciaires – V. *infra* n°642.
[1040] « Application des peines, probation et insertion (APPI) » prévu aux art. R57-4-1 et s. du C. pr. pén. – Le BIOAP créé par le décret n°2010-615 du 7 juin 2010 portant création de traitements automatisés de données à caractère personnel relatifs à l'identification biométrique des personnes écrouées, dénommés « BIOAP » - GIDE pour la gestion informatisée des détenus en établissement.

contiennent des données contribuant au suivi des dossiers. D'autres traitements ne sont pas mis en œuvre par les autorités judiciaires et contiennent pourtant des informations potentiellement utiles à l'avancée d'une enquête. Dans ce contexte de foisonnement de fichiers, les traitements judiciaires sont ceux qui répondent à deux critères. En premier lieu, ils sont directement accessibles par les autorités judiciaires, qui n'ont pas à utiliser une réquisition pour obtenir les données contenues dans ce traitement. En second lieu, leur consultation constitue une investigation numérique, puisque les informations qu'ils contiennent doivent potentiellement fournir des éléments de preuve, c'est-à-dire qu'elles sont susceptibles de faire progresser une procédure pénale.

629. Dès lors, c'est un nombre très important de traitements judiciaires qui répondent à ces critères et qui doivent être étudiés afin d'en déterminer les régimes qui permettent d'obtenir des données utiles à l'enquête.

Section 2. Les régimes des traitements judiciaires susceptibles de fournir des preuves

630. La nécessité d'une étude traitement par traitement. – Les traitements judiciaires sont éparpillés dans le Code de procédure pénale ainsi que dans une multitude de textes. Il en résulte une pluralité des régimes, notamment pour les conditions de leur consultation. De plus, l'impossibilité avérée d'en dresser une liste exhaustive complexifie leur étude. Dans ce contexte, il n'existe pas de classement logique et rigoureux de ces fichiers. Sur ce point, la situation est similaire aux actes intrusifs permettant l'obtention de données[1041]. Il n'existe donc pas d'autres solutions que de les étudier individuellement.

631. Une proposition de classement. – En conséquence, les seules tentatives de classement ne peuvent être que le fruit de réflexions doctrinales. Sur ce point, certains auteurs proposent une organisation efficace de ces différentes bases de données, en fonction de leur finalité, distinguée en fichiers de renseignement, d'identification, des condamnés et une catégorie pour les fichiers d'analyse sérielle et de rapprochement judiciaire[1042].

[1041] V. *supra* n°235.
[1042] *Op. cit.* p.20. SONTAG KOENIG Sophie, *Technologies de l'information et de la communication et défense pénale* : p. 99 et s.

632. Même si le raisonnement retenu ici est proche de ce classement par finalités, il est tout de même différent. En effet, le critère principal pour classer les traitements de données directement accessibles en enquête pénale repose, dans la présente étude, sur le degré d'exploitation informatique des données qui est légalement permis. Ce critère rejoint celui utilisé pour classer les actes intrusifs[1043]. Il s'agissait également de raisonner sur la donnée : à savoir la façon dont elles étaient obtenues[1044]. Cette caractéristique permet de distinguer les fichiers de consultation et ceux destinés à la corrélation des informations.

633. Les traitements judiciaires pour la consultation. – Ces derniers désignent des fichiers qui sont interrogés à partir du nom d'une personne afin d'obtenir, dans un premier temps, une réponse binaire (présente dans le fichier ou pas) et, dans un second temps, des informations liées au nom saisi si celui-ci est effectivement présent dans le fichier[1045]. Plus rarement, au sein des fichiers de consultation, certains traitements autorisent une consultation avec des mots clés différents des noms d'individus et permettent donc une exploitation plus performante et extensive des informations qu'ils contiennent. C'est notamment le cas avec des empreintes retrouvées sur une scène de crime et dont on ne sait pas à qui elles appartiennent[1046], ou encore des mots clés relatifs à un lieu ou un type de véhicule[1047], qui ont potentiellement pour résultats des informations qui, *in fine*, sont le plus souvent nominatives. Ainsi, à partir de critères de recherche techniques ou factuels, l'enquêteur peut obtenir, en réponse aux requêtes dans le fichier, un ou des noms de personnes, dont l'identité était peut-être totalement inconnue dans le dossier concerné jusque-là.

634. Les traitements judicaires pour la corrélation d'informations. – Les traitements destinés à la corrélation des informations constituent une gradation supplémentaire aux bases de données que l'on peut interroger sur des critères multiples. Dans cette hypothèse, l'agent ou le militaire utilise des algorithmes permettant des

[1043] V. *supra* n°235.
[1044] V. supra n°241.
[1045] Ex. : le fichier des personnes rercherchées. C. pr. pén. art. 230-19. Décret n°2010-569 du 28 mai 2010 relatif au fichier des personnes recherchées. V. *infra* n°655.
[1046] Ex. : le fichier national automatisé des empreintes génétiques (C. pr. pén. art. 706-54 et s. - C. pr. pén. art. R53-9 - V. *infra* n°661.). C. pr. pén. art. R53-10 : « […] Des traces biologiques issues de personnes inconnues, recueillies dans le cadre d'une enquête préliminaire, d'une enquête pour crime ou délit flagrant, ou d'une instruction préparatoire […]. »
[1047] Ex. : le Traitement d'antécédents judiciaires (C. pr. pén. art. 230-6 et s. v. *infra* n°642.).

recherches avancées sur les données, en procédant à des rapprochements et des recoupements. Un tel travail sur les informations n'est pas une consultation au sens informatique du terme, mais correspond à l'exploitation informatique d'une base de données[1048].

635. La nécessité d'organiser l'étude des traitements de données. – Outre la difficulté de proposer un classement pertinent, une étude détaillée de ces traitements de données peut rapidement se révéler rébarbative en raison d'une énumération fastidieuse de textes et de dispositions, qu'il est le plus souvent difficile de ne pas paraphraser. Aussi, les bases de données étudiées ci-après font, sauf indication contraire, l'objet d'une fiche normalisée permettant, tout d'abord, de visualiser rapidement leurs principales caractéristiques, dont les informations qui peuvent en être extraites, puis, par voie de conséquence, de les comparer rapidement.
Dans l'en-tête de ces fiches, il est indiqué si le traitement de données en question, est un traitement de consultation *(§1)* ou de corrélation des données contenues *(§2)*. L'ensemble de ces fiches sont regroupées en annexe des présentes[1049].

§1. Les traitements judiciaires pour la consultation

636. Des traitements mis en œuvre par des services administratifs non judiciaires. – Les fichiers pour la consultation permettent de savoir si une personne est présente dans une base de données[1050] particulière telle que le fichier des personnes recherchées ou d'être identifiée à partir de ses empreintes qui aurait été retrouvées sur une scène de crime. Ces fichiers peuvent aussi, à partir du nom d'une personne, fournir des renseignements personnels (dangerosité, condamnation antérieure, etc). Or, comme précédemment expliqué[1051], les autorités judiciaires bénéficient d'un accès direct[1052], légalement prévu, à des traitements autres que judiciaires. Il s'agit de bases de données administratives, mises en œuvre par d'autres services administratifs.

[1048] V. *infra* n°766.
[1049] V. annexe 1 : description et classification des fichiers et traitements de données judiciaires.
[1050] « Fichiers » et « bases de données » sont utilisés comme synonymes de « traitements judiciaires » dans la présente étude : v. *supra* n°609.
[1051] V. *supra* n°613.
[1052] Lorsque l'accès n'est pas explicitement prévu pour un traitement de données administratifs, les autorités judiciaires doivent utiliser le régime de la réquisition : v. *supra* n°372.

Il convient donc de distinguer l'étude des fichiers purement judiciaires *(I)*, et des bases de données administratives[1053] directement accessibles par les enquêteurs *(II)*.

I – Les bases de données judiciaires

637. La différence entre les traitements généralistes et spécialisés. – Le classement le plus clair pour les bases de données judiciaires repose sur leur finalité. En premier lieu, plusieurs traitements de données jouent un rôle prépondérant dans l'activité quotidienne des officiers de police judiciaire. Ils contiennent des informations sur le passé judiciaire[1054] d'une personne. Ces informations sont très générales puisqu'elles comportent, par exemple, le contexte d'une interpellation ou d'une audition, ou la déclaration d'un vol avec violence[1055]. En second lieu, d'autres traitements sont, au contraire, fortement spécialisés, comme le fichier judiciaire national automatisé des auteurs d'infractions terroristes[1056] ou le fichier des objets et des véhicules signalés[1057]. Ainsi, les traitements qui ont pour finalité d'informer les autorités judiciaires sur les antécédents d'un individu *(A)* et ceux qui sont consultés dans le cadre de recherches précises et ciblées en fonction du contexte des investigations*(B)* sont distingués.

A. Les traitements généraux d'antécédents judiciaires

638. L'importance du passé judiciaire des personnes. – Les enquêteurs accordent beaucoup d'importance au passé judiciaire d'un individu. La notion de « passé judiciaire » doit être entendue très extensivement car, au-delà de condamnations antérieures, les enquêteurs sont sensibles au simple fait que le nom d'une personne ait été évoqué dans un dossier précédent. Ces fichiers contiennent énormément d'informations, telles que les fréquentations d'une personne, s'il a récemment causé des troubles à l'ordre public, ou encore s'il possède un véhicule.

[1053] « Administratif » doit ici être entendu pour ses deux sens, à savoir aussi bien en référence à police ou enquête administrative, qu'en référence à la notion de traitements mis en œuvre par une administration.
[1054] Le mot « antécédents » est volontairement évité puisque celui-ci fait directement référence à l'un des traitements de données utilisés par les enquêteurs : le Traitement des Antécédents Judiciaires (TAJ).
[1055] VEDEL Renaud, *Le rôle des fichiers dans l'action opérationnelle des services de sécurité intérieure*, Dalloz AJ pénal 2007 p.64 : « Ils permettent par exemple de repérer le caractère sériel ou répété de certains actes de délinquance, d'effectuer des rapprochements relatifs aux horaires, aux lieux, aux modes opératoires ou au profil des auteurs ou de leurs victimes. »
[1056] V. *infra* n°667. C. pr. pén. art.706-25-3 et s. - C. pr. pén. art. R50-30 et s.
[1057] V. *infra* n°684. Arrêté du 17 mars 2014 portant autorisation à titre expérimental d'un traitement automatisé de données à caractère personnel dénommé « Fichier des objets et des véhicules signalés » (FOVeS).

639. Tout d'abord, dans leur travail de police judiciaire, les enquêteurs ont à leur disposition des traitements de données qui font partie de leurs outils de travail quotidien *(1)*, c'est-à-dire auxquels ils accèdent facilement car ceux-ci sont intégrés à leur environnement informatique. Ensuite, d'autres fichiers contiennent également des informations sur le passé judiciaire d'une personne, mais ne peuvent être consultés que selon un régime précisément défini *(2)*. Parfois, cette consultation est réservée à la poursuite de certaines infractions.

1. Les fichiers pour les enquêteurs au quotidien

☞ *V. annexe 1, fiches A1-1 et A1-2.*

640. Le paradoxe d'un traitement judiciaire majeur mais à l'utilité limitée pour l'enquête. – Le traitement judiciaire constituant la référence en matière de données ayant des sources pénales, est le Casier judiciaire[1058] qui existe depuis 1848. Celui-ci a une double utilisation. La première est « administrative[1059] » que l'on retrouve au travers des bulletins 2 et 3, car ceux-ci sont fréquemment nécessaires pour des dossiers qui demandent un extrait de casier[1060]. L'autre utilisation est judiciaire, par essence, avec le bulletin n°1. Celui-ci fournit les informations qui font foi en matière de condamnation. L'alimentation et la mise à jour du casier judiciaire font l'objet d'un suivi très rigoureux par un service qui lui est entièrement dédié.

641. Le rôle essentiel du service du Casier judiciaire. – Ce service joue un rôle de plus en plus important puisqu'il lui est confié la gestion de plusieurs autres fichiers sensibles[1061]. C'est en raison de ce positionnement comme structure de référence en matière de gestion de bases de données judiciaires qui tend à lui être confié, que le service du Casier judiciaire est intéressant.

642. Le traitement d'antécédents judiciaires : une source conçue au service des enquêteurs. – En effet, les données qui peuvent être extraites du Casier lui-même ne sont

[1058] V. **annexe 1, fiche A1/1.**
[1059] ROBERT Jacques-Henri, *Droit pénal général*, 5ième édition, Puf Droit, page 531 : « Longtemps, on a limité son usage à ce rôle subalterne et administratif […]. »
[1060] Exemple : recrutement dans la fonction publique ou pour des emplois dans des postes à risques comme la sureté nucléaire, le contrôle des bagages dans les aéroports (bulletin n°2), etc.
[1061] V. *infra* n°668. et 672.

pas susceptibles de constituer une investigation numérique véritablement efficace, car il est largement supplanté, en termes de contenu d'informations, par le traitement d'antécédents judiciaires (TAJ)[1062] mis en œuvre par les services de la Police et de la Gendarmerie.

643. En somme, le casier judiciaire est le document officiel qui est versé à la procédure, tandis que les enquêteurs exploitent, dans leur travail quotidien de police judiciaire, les informations issues du TAJ.

644. Le TAJ issu de la fusion de deux fichiers. – Historiquement, le traitement d'antécédents judiciaires est l'aboutissement d'un long processus[1063] qui a conduit à fusionner le STIC[1064] de la Police et le JUDEX[1065] de la Gendarmerie, après plusieurs étapes intermédiaires qui ont vu cette base de données centralisée s'appeler ARIANE puis « traitement des procédures judiciaires ». Le TAJ n'est réellement entré en pleine application qu'en 2015[1066]. Il est important d'évoquer ces différents noms, notamment ceux des deux traitements originels, car le TAJ est encore régulièrement désigné par le nom de STIC ou de JUDEX.

645. Une collecte très vaste d'informations. – Le traitement d'antécédents judiciaires est très riche en informations car il ne contient pas seulement les données des personnes condamnées, mais de toutes les personnes suspectées dans le cadre des enquêtes, ainsi que des victimes, sans oublier des données relatives aux personnes morales[1067]. De plus, au niveau des données collectées, outre le signalement et les photos de ces personnes, toutes les informations en lien avec l'enquête sont enregistrées, ce qui fait du TAJ un traitement particulièrement étendu en termes de données stockées.

646. Ses consultations[1068] constituent ainsi potentiellement des investigations numériques très performantes en raison de la richesse et de la transversalité des

---

[1062] V. **annexe1, fiche A1/2.**

[1063] SCHWENDENER Marc, *Police technique et scientifique*, Dalloz Répertoire de droit pénal et de procédure pénale, février 2019 : « […] il avait fallu attendre le décret no 2006-1411 du 20 novembre 2006 pour régulariser vingt années d'existence […]. »

[1064] Système de traitement des infractions constatées qui avait été créé par le décret n°2011-583 du 5 juillet 2001.

[1065] Système judiciaire de documentation et d'exploitation créé par le décret n°2006-1411 du 20 novembre 2006.

[1066] BAUER Alain et SOULLEZ Christophe, *Les fichiers de police et de gendarmerie, op. cit.* p.35.

[1067] C. pr. pén. art. R40-26.

[1068] Le pluriel est nécessaire puisqu'au cours d'une enquête, *a fortiori* complexe, les enquêteurs vont régulièrement l'interroger au fur et à mesure que de nouveaux noms apparaissent dans le dossier.

informations contenues[1069]. Il ressort des interviews réalisées dans le cadre des présents travaux, que le TAJ peut être interrogé au travers de mots clés autres que le nom d'individus et donc, par voie de conséquence, révéler des noms de personnes dont l'identité n'apparaissait pas jusque-là dans la procédure.

647. Une exploitation des données dépassant le cadre légal prévu. – L'exploitation du TAJ va plus loin encore, générant ainsi une confusion fortement dérangeante sur son positionnement en tant que logiciel de rapprochement judiciaire[1070]. En effet, de même que certains offices centraux se livrent à du développement sous *Windev* pour exploiter des données[1071], les enquêteurs spécialisés utilisent parfois des outils SQL pour réaliser des requêtes dans la base de données[1072]. On bascule ici clairement dans le cadre des traitements pour la corrélation d'informations[1073], ce qui est contraire aux dispositions légales et règlementaires, puisqu'en aucun cas le TAJ n'est déclaré en tant que fichier d'analyse sérielle ou de logiciel de rapprochement judiciaire.

648. Un accès administratif aux données du TAJ largement ouvert. – La perméabilité entre les informations judiciaires et administratives a considérablement été accrue au travers de la succession de textes pris en réaction suite à la vague d'attentats qu'ont connu la France et les autres pays européens. Désormais, la communication et l'accès par les autorités administratives aux informations judiciaires sont largement ouverts[1074]. La loi du 28 février 2017 a créé l'article 706-25-2 dans la Code de procédure pénale qui prévoit que « le procureur de la République de Paris, pour les procédures d'enquête ouvertes sur le fondement d'une ou de plusieurs infractions [terroristes], peut communiquer aux services spécialisés de renseignement […], de sa propre initiative ou à la demande de ces services, copie des éléments de toute nature figurant dans ces procédures et nécessaires à l'exercice des missions de ces services en matière de

[1069] V. *infra* n°995. En 2013, le fichier des antécédents contenait 12,2 millions de fiches de personnes mises en cause.
[1070] V. *infra* n°720.
[1071] V. *supra* n°616.
[1072] Les requêtes SQL sont utilisées par les informaticiens pour extraire des informations depuis une base de données. Il s'agit d'une sorte de langage de programmation qui permet d'interroger la base de données beaucoup plus efficacement qu'avec les outils normalement offerts aux utilisateurs du TAJ.
[1073] V. *supra* n°634.
[1074] FOURMENT François, *Sécurité intérieure – La loi n°2017-258 du 28 février 2017 relative à la sécurité publique dans ses aspects de droit pénal,* LexisNexis, Droit pénal n°5, mai 2017 : « Communication, par l'autorité judiciaire, d'informations en matière de prévention du terrorisme aux services de renseignement. »

prévention du terrorisme ». Or, cet article 706-25-2 n'est qu'une possibilité relativement encadrée de communication d'éléments judiciaires aux autorités administratives. Le décret du 2 août 2017[1075] a considérablement étendu de telles possibilités en venant, notamment, modifier l'article R40-29 et créer l'article R40-29-1 du Code de procédure pénale, permettant ainsi une consultation à des fins administratives du TAJ, et ceci « sans autorisation du ministère public[1076] ».

649. Une base de données pour les procès-verbaux. – Toujours dans la catégorie des applications supports de l'activité quotidienne de police judiciaire de la Gendarmerie et de la Police nationales, les deux logiciels LRPPN[1077] et LRPGN[1078] servent à la rédaction des procès-verbaux et sont donc le support des échanges avec les magistrats, qu'ils soient du Parquet ou de l'instruction. Subséquemment, on notera que contrairement au traitement d'antécédents judiciaires où la volonté de faire converger le système d'information de la Police et de la Gendarmerie s'est concrétisée, cela n'est pas le cas ici où la dichotomie qui existait avec ARDOISE[1079] et ICARE[1080] a été maintenue avec le LRPPN et le LRPGN. D'ailleurs, il est étrange que les données appelées à être collectées dans le LRPPN soient beaucoup plus étoffées que celles du LRPGN[1081]. Les fonctionnalités exactes annoncées pour ces deux logiciels sont de collecter et d'archiver les informations recueillies lors des missions de police judiciaire ou administrative (données issues de procès-verbaux, comptes rendus d'enquêtes et rapports administratifs ou judiciaires), la réalisation de statistiques et, à terme, d'alimenter le TAJ.

650. Ainsi, aucune fiche dédiée n'est jointe en annexe 1 pour ces deux traitements car ils sont moins riches en informations[1082] que le TAJ et en sont très proches pour le reste des données susceptibles de fournir des éléments à une enquête ultérieure. En revanche, ils sont essentiels en raison du rôle d'échange d'informations qui est prévu avec les

[1075] Décret n°2017-1217 du 2 août 2017 modifiant le traitement d'antécédents judiciaires.
[1076] C. pr. pén. art. R40-29, I.
[1077] Logiciel de rédaction des procédures de police nationale (LRPPN). Décret n°2011-110 du 27 janvier 2011 portant création d'un traitement automatisé de données à caractère personnel dénommé LRPPN.
[1078] Logiciel de rédaction des procédures de gendarmerie nationale (LRPGN). Décret n°2011-111 du 27 janvier 2011 autorisant la mise en œuvre par le ministère de l'intérieur (direction générale de la gendarmerie nationale) d'un traitement automatisé de données à caractère personnel d'aide à la rédaction des procédures (LRPGN).
[1079] Application de recueil de la documentation opérationnelle et d'informations statistiques sur les enquêtes (ARDOISE) pour la Police nationale.
[1080] Gendarmerie nationale
[1081] V. *infra* n°652.
[1082] Par exemple, les photos d'identification ne sont pas prévues dans le LRPPN et le LRPGN.

magistrats. A terme, le LRPPN et le LRPGN doivent alimenter le TAJ pour les données d'identification des personnes et pour garantir l'homogénéité des numéros de procédures.

651. Tout comme pour le TAJ[1083], ces deux bases de données prévoient que les informations relatives aux faits soient des points d'entrée de la consultation du traitement[1084]. Cela signifie que les recherches au sein de ces deux fichiers ne sont pas limitées sur des noms de personnes. Des mots clés relatifs aux faits peuvent être utilisés pour interroger les bases.

652. Pour le LRPPN, l'annexe au décret du 27 janvier 2011 dispose que peuvent être saisies les données relatives aux « faits objet de l'enquête, les lieux, la date de l'infraction, ainsi que les informations relatives aux objets, y compris celles qui sont indirectement nominatives ». La précision sur les données « indirectement nominatives » est très instructive car elle explicite qu'une recherche dont les mots clés sont relatifs aux faits, peuvent avoir pour résultat des noms d'individus.

653. Conclusion du sous-paragraphe 1 : les fichiers pour les enquêteurs au quotidien. – L'environnement de travail informatique quotidien des enquêteurs intègre différents traitements judiciaires. Ils sont créés le plus souvent par voie règlementaire, au travers de décrets non codifiés. Il en résulte un éparpillement des textes encadrant ces outils, engendrant des régimes différents, notamment pour leur utilisation et les transferts de données autorisés. L'éparpillement des régimes encadrant ces fichiers est accentué par le fait que des dispositions les concernant sont présentes dans le Code de procédure pénale, alors que les règles générales sont définies dans le décret dédié à sa création. Les données qui peuvent être extraites lors de la consultation de ces traitements sont très vastes. De plus, les manipulations réellement réalisées par les enquêteurs dépassent nettement le cadre règlementaire originel[1085].

[1083] V. *supra* n°646.

[1084] Décret n°2011-110 du 27 janvier 2011 portant création d'un traitement automatisé de données à caractère personnel dénommé LRPPN, art. 1 : « […] De permettre la collecte des informations issues de ces procédures, en vue […] de leur exploitation ; »
Décret n°2011-111 du 27 janvier 2011 autorisant la mise en œuvre par le ministère de l'intérieur (direction générale de la gendarmerie nationale) d'un traitement automatisé de données à caractère personnel d'aide à la rédaction des procédures (LRPGN), art. 5 : « […] Peuvent accéder, à raison de leurs attributions et dans la limite du besoin d'en connaître, à tout ou partie des données et informations mentionnées à l'article 2, les militaires ainsi que les agents de la police nationale […]. »

[1085] V. par ex. les recherches directement opérées dans la base de données du TAJ, v. *supra* n°647.

Outre les traitements judiciaires directement intégrés dans les outils de travail quotidiens des enquêteurs, il existe des bases de données contenant des informations spécifiques, également issues du passé judiciaire des individus fichés.

2. Les fichiers relatifs au passé judiciaire des individus

654. Des traitements spécialisés sur des typologies d'informations. – Un ensemble de traitements judiciaires a pour finalité principale d'enregistrer et de prendre en compte certaines spécificités du passé judiciaire des personnes qui y sont inscrites.
Tout d'abord, un premier ensemble de traitements sert à attirer l'attention des forces de l'ordres lorsqu'elles sont confrontées à un individu donné et, plus généralement, vise à faciliter la recherche de personnes *(a)*.
Ensuite, plusieurs bases de données sont destinées à identifier des individus, le plus souvent dangereux *(b)*.

a. La recherche d'individus

☞ *V. annexe 1, fiches A1-3 et A1-4.*

655. La perception très extensive de la notion de « personnes recherchées ». – Les informations susceptibles d'être collectées dans le fichier des personnes recherchées[1086] sont particulièrement vastes[1087]. Outre les personnes inscrites au fichier qui peuvent être regroupées dans la catégorie « recherchées suite à une décision judiciaire », l'inscription de « personnes faisant l'objet d'une mesure administrative d'interdiction de stade », de personnes ayant fait l'objet d'une interdiction de manifester[1088], de personnes ayant fait l'objet d'un retrait de permis de conduire ou encore d'individus frappés d'une interdiction d'exercer certaines activités, soulève une interrogation quant à l'adéquation entre l'intitulé de ce traitement et les données effectivement collectées.
656. La finalité de telles inscriptions est aisée à comprendre : elle vise à renforcer l'efficacité des contrôles de police et de gendarmerie (qu'ils soient dans le cadre d'une procédure judiciaire ou, plus fréquemment, administratifs), notamment en détectant

[1086] V. **annexe 1, fiche A1/3.**
Décret n°2010-569 du 28 mai 2010 relatif au fichier des personnes recherchées.
[1087] *Ibid.* V. art. 2 du décret.
[1088] LETTERON Roseline, *Les débris de la loi « anti-casseurs »*, Dalloz AJ pénal 2019 p.259 : « Il subsiste comme un élément du fichier des personnes recherchées, mais ne peuvent y être conservés que les noms des personnes faisant l'objet d'une interdiction pénale de manifester. »

instantanément une violation d'une décision de justice. Pour autant, on ne peut que s'étonner du respect des libertés individuelles en étendant les finalités d'un traitement de données de manière totalement incohérente avec sa désignation.

657. Ainsi, une personne inscrite dans le fichier, peut se voir qualifiée de « personne recherchée », alors qu'elle ne fait l'objet d'aucune décision judiciaire, et se retrouver assimilée à des individus faisant l'objet, par exemple, d'un mandat délivré par une juridiction d'instruction[1089]. Un tel enregistrement semble difficilement compatible avec le respect des libertés individuelles et, tout particulièrement les articles 6 et 8 de la Convention européenne de sauvegarde des droits de l'homme[1090].

658. Les traitements issus du bracelet électronique. – Dans la continuité de la recherche d'individu, il convient de revenir sur les dispositifs de surveillance mobiles dont le régime est décrit au sein des actes intrusifs d'obtention de données[1091]. L'utilisation de ces dispositifs est, en effet, rendue possible grâce à la création de traitements de données à caractère personnel. Deux fichiers sont ainsi créés pour correspondre aux deux types de surveillance mobile auxquelles il est possible de procéder[1092]. Comme précédemment indiqué[1093], le placement sous surveillance électronique (PSE) ne présente pas d'intérêt en tant qu'investigation numérique[1094], puisque seules les données d'entrée et de sortie dans la zone assignée sont enregistrées, et ceci même si un accès aux données est prévu en enquête[1095]. En effet, les informations de géolocalisation en dehors de la zone d'assignation ne sont pas collectées[1096].

659. En revanche, le placement sous surveillance électronique mobile (PSEM) possède un potentiel très intéressant en matière d'investigation numérique comme cela est étudié dans le cadre des investigations numériques intrusives par action. Le traitement de données correspondant[1097] prévoit un accès au stade de l'enquête[1098], aux fins de connaître la localisation de la personne surveillée. L'intérêt réside ici dans le fait qu'il offre la

[1089] C. pr. pén. art. 122 : mandat de recherche, de comparution, d'amener ou d'arrêt.
[1090] Sur le respect des libertés individuelles, v. *supra* n°313.
[1091] V. *supra* n°517.
[1092] PSE et PSEM : *ibid.*
[1093] *Ibid.*
[1094] La base de données correspondante est le « traitement automatisé de données à caractère personnel relatif au contrôle des personnes placées sous surveillance électronique » prévue aux art. R57-30-1 et s. du C. pr. pén.
[1095] C. pr. pén. art. R57-30-2 4°).
[1096] V. *supra* n°519.
[1097] V. **annexe 1, fiche A1/4** - C. pr. pén. art. R61-12 et s.
[1098] C. pr. pén. art. R61-12, 4ème alinéa, 3°).

possibilité aux enquêteurs d'obtenir des éléments factuels sur la présence d'un suspect en un lieu précis et à un moment donné.

b. L'identification d'individus et de leur dangerosité

☞ *V. annexe 1, fiches A1-5 à A1-9.*

660. Des traitements judiciaires fortement spécialisés. – L'Etat a éprouvé le besoin de créer un ensemble de traitements de données destinés à stocker des informations permettant d'identifier des personnes à partir de traces biologiques *(α)* qui pourraient être retrouvées ou, dans le cas où le nom de telles personnes viendrait à apparaitre dans un dossier, d'extraire des informations sur leur dangerosité en fonction de typologies criminelles particulières *(β)*.

α. L'identification par des traces biologiques

661. Deux fichiers complémentaires. – La génétique prend aujourd'hui de plus en plus de place dans les enquêtes ce qui, bien sûr, met particulièrement sur le devant de la scène « le fichier national automatisé des empreintes génétiques[1099] », au risque de reléguer « le fichier automatisé des empreintes digitales[1100] » au rang des techniques d'identification archaïques. C'est toutefois une vision erronée car ce procédé reste facile à mettre en œuvre, peu couteux à côté de la recherche et de la gestion des empreintes génétiques et, surtout, possède une base de données bien plus riche en raison de son antériorité.

662. Ces deux traitements ont une spécificité qui mérite d'être soulignée. En effet, la base de données contient, fort logiquement, des noms de personnes associés à leurs empreintes, mais également des empreintes complètes ou partielles qui ont été relevées sur des scènes de crime et dont on ne sait pas à qui elles appartiennent. Ainsi, si une empreinte identique est retrouvée sur une nouvelle scène de crime, cela permet d'établir un lien entre les différentes affaires ou, dans une situation idéale, si un suspect est arrêté

[1099] V. **annexe 1, fiche A1/6.**
Décret n°2004-470 du 25 mai 2004 modifiant le code de procédure pénale (deuxième partie : Décrets en Conseil d'Etat) et relatif au fichier national automatisé des empreintes génétiques.
PASCAL Olivier et SCHLENK Alexandra, *L'empreinte génétique : le spectre de la preuve absolue*, Dalloz AJ pénal 2004 p.24.
[1100] V. **annexe 1, fiche A1/5.**
Décret n°87-249 du 8 avril 1987 relatif au fichier automatisé des empreintes digitales géré par le ministère de l'intérieur.

et que ses empreintes correspondent à celles d'un dossier antérieur, une procédure précédemment bloquée se trouve relancée[1101].

663. Une forme de « délit » de parenté. – Les empreintes génétiques offrent une puissance d'investigation que ne permettent pas les empreintes digitales. C'est pourquoi la loi du 3 juin 2016[1102] a autorisé la comparaison d'une « trace biologique issue d'une personne inconnue[1103] » avec les données enregistrées dans le fichier, afin de déterminer si cet individu non identifié n'a pas un lien de parenté avec une personne fichée. Comment doit-on interpréter cette disposition ? Est-ce que cela fait peser sur le frère ou le parent d'un criminel ou d'un délinquant une présomption de culpabilité ? Est-ce que les statistiques démontrent que la grande criminalité ou le terrorisme s'exerce en famille ? On comprend que l'objectif est ici d'améliorer la performance de l'identification d'une personne inconnue ayant laissée des traces sur une scène de crime, mais il est choquant pour un pays démocratique de créer un « soupçon familial » au travers d'une disposition laconique qui n'encadre quasiment pas le recours à cette recherche[1104].

664. D'ailleurs, il est intéressant de noter que la France a déjà fait l'objet d'une condamnation par la CEDH[1105] relative au fichier des empreintes génétiques. Dans cette décision de 2017, la Cour a estimé « que le régime actuel de conservation des profils ADN […] n'offre pas, en raison tant de sa durée que de l'absence de possibilité d'effacement, une protection suffisante […] ». De plus, le nouvel article 95 de la loi informatique et libertés[1106] prohibe « tout profilage qui entraîne une discrimination à l'égard des personnes physiques sur la base de catégories particulières de données à caractère personnel mentionnées au I de l'article 8 est interdit ». La référence au « I de l'article 6 » de la loi informatique et libertés vise explicitement les données génétiques.

[1101] V. par ex. Le Parisien, *Le mystère des bébés de Galfingue élucidé 14 ans après*, 1er décembre 2017. Des bébés morts avaient été retrouvés en 2003 sans que l'on puisse les identifier. En 2013, les investigations avaient été rouvertes précisément pour opérer des prélèvements ADN. C'est au détour de faits totalement étrangers à ce dossier que le fichier des empreintes génétiques a été consulté et a permis de retrouver la mère des bébés.

[1102] Loi n°2016-731 du 3 juin 2016. *Op. cit.* p.23

[1103] C. pr. pén. art. 706-56-1-1.

[1104] *Ibid.* « Lorsque les nécessités d'une enquête ou d'une information concernant l'un des crimes prévus à l'article 706-55 l'exigent […]. »

[1105] CEDH 22 juin 2017 Aycaguer c. France.

[1106] Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par l'ordonnance n°2018-1125 du 12 décembre 2018 prise en application de l'article 32 de la loi n°2018-493 du 20 juin 2018 relative à la protection des données personnelles et portant modification de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et diverses dispositions concernant la protection des données à caractère personnel.

De plus, la définition du « profilage[1107] » montre le lien entre ce terme et les « indices recueillies par les services d'enquête » dont font explicitement partie les informations extraites du fichier national automatisé des empreintes génétiques.

665. Une contrepartie trop mince pour assurer la protection des personnes. – Néanmoins, l'article R53-11 du Code de procédure pénale prohibe explicitement la recherche par des mots clés « sur la nature de l'affaire », ce qui démontre qu'il s'agit uniquement d'un traitement judiciaire de consultation[1108] et que toute investigation dans le fichier avec des recherches sur des données autres que des noms ou des empreintes est exclue pour ce traitement. Pour autant, cette limitation n'est pas suffisante pour protéger les personnes face à la latitude de consultation autorisée pour ce traitement.

666. Conclusion du sous-paragraphe *α* : l'identification par des traces biologiques. – Les deux bases de données relatives aux empreintes, aussi bien génétiques que digitales, sont avant tout des fichiers permettant d'identifier des individus. Des traitements, tout aussi spécialisés, ont pour finalité d'indiquer le degré potentiel de dangerosité d'une personne.

β. L'identification par le degré de dangerosité

667. Deux fichiers regroupant des infractions graves. – Deux traitements de données créés et gérés par les institutions judiciaires s'intéressent à des infractions particulièrement graves : le « fichier national automatisé des auteurs d'infractions sexuelles ou violentes[1109] » et le « fichier judiciaire national automatisé des auteurs d'infractions terroristes[1110] ».

668. L'aspect sensible des données qui y sont contenues fait que les deux bases de données sont gérées par le service du Casier judiciaire, ce qui illustre, outre une notion économique évidente de mutualisation des ressources techniques et humaines dans la

[1107] Source Larousse : « En criminologie, établissement du profil psychologique d'un individu recherché (tueur en série, notamment), en fonction des indices recueillis par les services d'enquête. »
[1108] V. *supra* n°633.
[1109] V. **annexe 1, fiche A1/7** – C. pr. pén. art. 706-53-1 et s. et R53-8-1 et s.
[1110] V. **annexe 1, fiche A1/8**. Décret n°2015-1840 du 29 décembre 2015 modifiant le code de procédure pénale et relatif au fichier judiciaire national automatisé des auteurs d'infractions terroristes.
THOMAS-TAILLANDIER Delphine, *Le nouveau fichier national des auteurs d'infractions terroristes*, Dalloz AJ pénal 2015 p.523.

mise en œuvre opérationnelle de ces traitements, une volonté d'en confier la gestion à une structure expérimentée.

669. Des recherches par mots clés autorisées. – Ces deux fichiers comportent des données vastes avec, notamment, tout ce qui est relatif à la procédure à l'origine de l'inscription de la personne[1111] et sont très intéressants d'un point de vue investigation numérique car les recherches par mots clés variés, c'est-à-dire dépassant les interrogations par le seul nom d'individu, sont explicitement autorisées[1112].

670. Une finalité dépassant la dénomination du traitement. – Tout comme pour le fichier des personnes recherchées[1113], le fichier national automatisé des auteurs d'infractions sexuelles ou violentes regroupe des finalités différentes. En effet, les infractions « sexuelles » et « violentes » ne correspondent pas nécessairement à la même typologie criminelle[1114]. Ce regroupement de plusieurs finalités dans un seul traitement est suffisamment rare pour être noté, puisque la tendance générale de l'Etat et du législateur est plutôt de spécialiser les fichiers, surtout lorsqu'il n'y a pas un lien direct entre les finalités regroupées.

671. Dans le cas présent, la loi a prévu qu'il puisse exister des infractions d'agressions sexuelles sans qu'elles soient systématiquement accompagnées de violences physiques. C'est notamment le cas du viol qui peut être commis par le biais de pressions uniquement psychologiques[1115]. Les infractions pour torture ou actes de barbarie conduisent également à l'inscription dans cette base de données, ce qui confirme le regroupement de deux types de dangerosité bien différentes.

672. Un fichier dédié au suivi de la dangerosité dans le temps. – Un dernier fichier concerne le suivi de l'évolution de la dangerosité de personnes condamnées. Il s'agit du REDEX[1116]. Il est également tenu par le service du Casier judiciaire. On ne peut qu'être

---

[1111] V. resp. C. pr. pén. art. R53-8-7 et R50-36.
[1112] V. resp. C. pr. pén. art. R53-8-23 et R50-51.
[1113] V. *supra* n°655.
[1114] HERZOG-EVANS Martine, *Les dispositions relatives à la récidive dans la loi n° 2005-1549 du 12 décembre 2005*, — Recueil Dalloz 2006. 182
[1115] V. C. pén. art. 222-24 : « Lorsqu'il est commis par un ascendant ou par toute autre personne ayant sur la victime une autorité de droit ou de fait » ou encore « lorsqu'il est commis par une personne qui abuse de l'autorité que lui confèrent ses fonctions. »
[1116] V. **annexe 1, fiche A1/9** – C. pr. pén. 706-56-2.
Décret n°2016-1338 du 7 octobre 2016 modifiant le Code de procédure pénale et relatif au répertoire des données collectées dans le cadre d'une procédure judiciaire.

interpellé par le fait que des individus objets du traitement sont, certes, les personnes condamnées, mais également celles poursuivies[1117]. Ainsi, quelqu'un qui est encore présumé innocent, peut voir toutes ses expertises psychiatriques et psychologiques enregistrées dans le REDEX au côté de délinquants multirécidivistes (le REDEX a, avant tout, été créé pour prévenir la récidive).

673. En revanche, un aspect positif pour la préservation de la sécurité publique, est que des personnes poursuivies mais n'ayant pas été condamnées en raison d'une irresponsabilité pénale reconnue[1118] sont enregistrées dans le fichier[1119].

674. Cette base de données présente peu d'intérêt pour les investigations numériques car la majorité des personnes fichées sont en détention. Pour que les données soient utiles, il faut imaginer qu'un individu fasse l'objet d'une libération, notamment conditionnelle, et se retrouve impliqué dans des faits délictueux ou criminels.

675. Conclusion du sous-paragraphe A : les traitements généraux d'antécédents judiciaires. – Ces traitements judiciaires sont totalement éparpillés dans une multitude de textes. Alors que les traitements intégrés aux outils informatiques quotidiennement utilisés par les enquêteurs sont créés par voie règlementaire, des bases de données considérées comme plus sensibles sont encadrées par des dispositions légales présentes dans le Code de procédure pénale[1120]. Il en découle de nombreux régimes différents, aussi bien dans la mise en œuvre de ces traitements que dans leur fonctionnement. La complexité qui en résulte permet de faire passer inaperçue deux problèmes majeurs qui entourent ces fichiers. En premier lieu, les dénominations de certains traitements judiciaires, comme le fichier des personnes recherchées ou le fichier national automatisé des auteurs d'infractions sexuelles ou violentes, ne sont pas cohérentes avec les informations collectées. En second lieu, l'utilisation qui est réellement faite des données stockées dans ces fichiers dépasse parfois le cadre règlementaire prévu, comme avec le traitement d'antécédents judiciaires.

[1117] C. pr. pén. art. R53-21-2 qui entre en vigueur le 1er mars 2018.
[1118] C. pén. art. 122-1.
[1119] V. C. pr. pén. art. 706-56-2 : « En cas de décision de classement sans suite, hormis les cas où cette décision est fondée sur le premier alinéa de l'article 122-1 du code pénal, ou de décision définitive de non-lieu, de relaxe ou d'acquittement, les données concernant la personne poursuivie sont immédiatement effacées. »
[1120] Ex : le fichier national automatisé des empreintes génétiques. V. *supra* n°661.

676. Au sein des bases de données purement judiciaires, il existe une autre catégorie de traitements pour les antécédents judiciaires, qui sont consultés dans le cadre de recherches spécifiques, directement liées à un contexte particulier.

B. Les traitements exploités dans des investigations spécialisées

677. L'obtention d'informations précises depuis des fichiers judiciaires non dédiés aux enquêtes. – Lorsqu'ils sont dans une phase intense d'investigation, les enquêteurs recherchent des informations partout où ils le peuvent. Tout d'abord, les traitements de données tels que l'ensemble des fichiers qui découlent indirectement du Code de la route peuvent être utiles *(1)*. Même s'ils n'ont pas été créés spécialement pour des enquêtes judiciaires, ils peuvent contenir des informations précieuses, notamment en révélant la présence horodatée d'un individu à un endroit déterminé. Ensuite, deux traitements de données découlent directement de la mise sous surveillance des suspects *(2)*.

1. Les fichiers pour les véhicules et leur circulation

☞ *V. annexe 1, fiches A1-10 et A1-11.*

678. Les traitements découlant des infractions liées aux véhicules. – Un ensemble de fichiers concernent les infractions au Code de la route ou sont en rapport direct avec les véhicules. Dans le présent paragraphe, seuls les fichiers judiciaires sont étudiés. Il existe également des traitements administratifs tel que le registre des cartes grises, pour lesquels un accès est explicitement réservé aux enquêteurs au cours des procédures pénales. Ceux-ci sont évoqués ultérieurement[1121].

679. Au premier abord, des données relatives aux infractions du Code de la route peuvent sembler peu pertinentes en tant qu'investigation numérique. Pourtant, dans certaines procédures, il est essentiel de reconstituer le trajet d'un individu[1122], ou d'un véhicule dont on sait qu'il a été utilisé lors d'une infraction : les données extraites de tels traitements peuvent alors se révéler essentielles, notamment si le véhicule a été flashé par un radar automatique[1123] ou s'il y a eu un contrôle des gendarmes qui s'est soldé par un

[1121] V. *infra* n°697.
[1122] V. par ex. OGER Lionel, *Prison ferme pour les voleurs,* La Nouvelle République, 23 oct. 2003 : « C'est ainsi que […] a été reconnu grâce à une photo radar. Tous les passagers de la R25 « flashée » étaient encagoulés, mais lui était assez facilement identifiable. »
[1123] Arrêté du 13 octobre 2004 portant création du système de contrôle automatisé.

procès-verbal[1124]. En fait, la Gendarmerie s'appuie sur l'application PULSAR[1125] qui repose sur ce traitement pour la gestion des amendes forfaitaires, associé à un autre traitement dénommé « Gestion des MIS et des BAA des unités[1126] ». La consultation de ce dernier ne peut pas constituer une investigation numérique, car les bases de données des « messages d'information statistique (MIS) » et des bulletins d'analyse des accidents (BAA) sont à vocation statistiques et d'études.

680. La lecture automatique des plaques d'immatriculation. – En revanche, un autre traitement relatif aux véhicules peut constituer une investigation numérique intéressante en permettant de connaître leur position à un instant donné. Celui-ci n'est pas directement lié à la constatation des infractions. Il s'agit du « traitement automatisé de contrôle des données signalétiques des véhicules[1127] » qui consiste à installer des dispositifs pour lire automatiquement les plaques d'immatriculation des véhicules en circulation ou en stationnement (dans ce cas le dispositif est embarqué dans un véhicule en mouvement) et d'en constituer une base de données avec une courte durée de conservation[1128]. L'objectif est clairement de faire du rapprochement avec d'autres fichiers judiciaires et administratifs afin de localiser une personne ou un véhicule recherché et donc de pouvoir déclencher des actions.

681. La vocation pénale de ce traitement de données est énoncée sans ambiguïté, puisqu'il est question de « constater » et de « réprimer » des infractions dont celles en lien avec le terrorisme ou la criminalité organisée[1129].

[1124] Arrêté du 2 décembre 2010 autorisant la mise en œuvre d'un traitement automatisé d'information à caractère personnel pour la gestion des amendes forfaitaires et des consignations dénommé « Gestion des amendes forfaitaires des unités élémentaires de la gendarmerie départementale et des gendarmeries spécialisés »

[1125] CNIL, délibération n°2010-117 du 6 mai 2010 portant avis sur le projet d'arrêté autorisant la mise en œuvre d'un traitement automatisé de données à caractère personnel dénommé « Gestion des amendes forfaitaires des unités élémentaires de la gendarmerie départementale et des gendarmeries spécialisées » qui émet un avis sur l'application PULSAR.

[1126] Arrêté du 2 décembre 2010 autorisant la mise en œuvre d'un traitement automatisé de données à caractère personnel pour la gestion des messages d'information statistique et des bulletins d'analyse des accidents des unités élémentaires de la gendarmerie départementale et des gendarmeries spécialisées dénommé « Gestion des MIS et des BAA »

[1127] V. **annexe1, fiche A1/10.**
Arrêté du 18 mai 2009 portant création d'un traitement automatisé de contrôle des données signalétiques des véhicules.

[1128] De 8 jours à 1 mois sauf si, bien sûr, les données deviennent utiles à une procédure pénale.

[1129] Article 1 de l'arrêté du 18 mai 2009 : « afin de permettre le rassemblement des preuves de ces infractions et la recherche de leurs auteurs. »

682. Une incohérence avec le Code de la sécurité intérieure. – Il est regrettable que ce traitement prévu depuis 2009 par l'arrêté du 18 mai, ait vu des dispositions quasi-similaires être introduites dans le Code de la sécurité intérieure par une ordonnance du 12 mars 2012[1130], sans qu'aucune cohérence ne soit établie entre les articles L233-1 et suivants résultants de l'ordonnance du 12 mars et l'arrêté du 18 mai 2009. Les finalités sont reprises dans le Code de la sécurité intérieure, y compris celles relatives à la constatation des infractions pénales. En revanche, il existe un grand flou quant à savoir ce que deviennent les données collectées en application de l'article L233-1 puisqu'il est indiqué que « pour les finalités mentionnées à l'article L233-1, les données à caractère personnel collectées à l'occasion des contrôles susmentionnés peuvent faire l'objet de traitements automatisés mis en œuvre par les services de Police et de Gendarmerie nationales et les services des douanes et soumis aux dispositions de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés[1131] ».

683. Nulle part ne sont définis les « traitements automatisés » évoqués. On imagine qu'en raison de la nature « administrative » qu'ont tenté de lui donner les pouvoirs publics, ils sont soumis aux régimes dérogatoires de la loi informatique et libertés[1132]. L'incohérence atteint son paroxysme avec les durées de conservation. En effet, les données enregistrées en vertu des dispositions du Code de la sécurité intérieure peuvent être conservées plus longtemps[1133] que celles collectées en application de l'arrêté de 2009.

684. Les fichiers relatifs aux véhicules déclarés volés. – Deux autres traitements sont relatifs aux véhicules volés. Le premier est « la base satellite des véhicules volés[1134] » dont la finalité principale est de mettre sous surveillance un véhicule volé qu'un individu tenterait de réintroduire dans le parc légal par le biais d'une opération d'immatriculation classique, ou qui ferait l'objet d'une contravention enregistrée dans l'un des fichiers qui viennent d'être décrits. La vocation de ce fichier est de mettre à disposition, notamment, des agents des services d'immatriculation des préfectures une base leur permettant de prévenir immédiatement l'enquêteur qui a mis le véhicule en question sous surveillance, en l'inscrivant dans ce fichier. C'est pour cette raison que la CNIL, dans la demande

[1130] Ordonnance n°2012-351 du 12 mars 2012 relative à la partie législative du code de la sécurité intérieure.
[1131] C. séc. int. art. L233-2.
[1132] V. *supra* n°613.
[1133] 15 jours contre 8 jours.
[1134] Arrêté du 10 décembre 2008 portant création par le ministère de l'intérieur d'un traitement automatisé de données à caractère personnel dénommé « base satellite VV ».

d'avis dont elle avait été saisie préalablement à la mise en œuvre du traitement, avait souhaité que le mot « accéder » soit indiqué comme finalité pour les destinataires principaux de cette base de données et non pas « enregistrer[1135] ».

685. En conséquence, ce fichier ne présente pas beaucoup d'intérêt en tant qu'investigation numérique car les données relatives au véhicule surveillé sont appelées à être inscrites dans une autre base de données, dont l'interrogation est potentiellement beaucoup plus pertinente pour une enquête : le fichier des objets et des véhicules signalés volés[1136]. Celui-ci est appelé à remplacer le fichier des véhicules volés[1137], en étendant fortement son périmètre à toute sorte d'objets volés (y compris les animaux) ou perdus. L'investigation numérique qui consiste à interroger ce traitement de données est importante car toutes les informations sur le contexte autour du vol, les photos de la chose volée, mais également tout ce qui touche à la découverte ultérieure de l'objet ou du véhicule volé sont enregistrés. En quelque sorte, cette base de données est équivalente au fichier des personnes recherchées[1138], transposé aux objets et aux véhicules.

2. Les fichiers créés lors de la mise sous surveillance d'individus

☞ *V. annexe 1, fiches A1-12 et A1-13.*

686. Les traitements créés pour la mise en œuvre d'actes de surveillance. – Au sein des traitements spécialisés susceptibles de fournir des informations précieuses aux enquêteurs dans des situations particulières, deux mesures de surveillance faisant partie des actes intrusifs permettant l'obtention d'informations numériques, ont une correspondance avec des traitements de données qui leur sont dédiés.

Il s'agit, d'une part, de la PNIJ qui met en œuvre les interceptions de correspondances[1139] *(a)* et, d'autre part, des traitements découlant de la captation des données[1140] *(b)*.

[1135] CNIL, délibération n°2008-381 du 23 octobre 2008 portant avis sur un projet d'arrêté du Ministère de l'intérieur, de l'outre-mer et des collectivités territoriales relatif à la création d'un traitement automatisé de données à caractère personnel dénommé « base satellite des véhicules volés » (BSVV).

[1136] V. **annexe 1, fiche A1/11.**
Arrêté du 17 mars 2014 portant autorisation à titre expérimental d'un traitement automatisé de données à caractère personnel dénommé « Fichier des objets et des véhicules signalés » (FOVeS).

[1137] Arrêté du 15 mai 1996 relatif au fichier des véhicules volés géré par le ministère de l'intérieur et le ministère de la défense, modifié par l'arrêté du 2 septembre 2005 pris pour l'application des articles 22 à 24 et 27 de la loi n°2003-239 du 18 mars 2003 modifiant l'arrêté du 15 mai 1996 relatif au fichier des véhicules volés géré par le ministère de l'intérieur et le ministère de la défense.

[1138] V. *supra* n°655.

[1139] V. *supra* n°528.

[1140] V. *supra* n°570.

a. Le fichier des écoutes téléphoniques

687. La double identité de la PNIJ. – La plate-forme nationale des interceptions judiciaires (PNIJ) présente la caractéristique d'être à la fois un traitement de données dument déclaré[1141], et une structure physique dotée de compétences humaines, d'outils techniques, et d'un cadre légal imposant[1142] et normalisant la collaboration avec les opérateurs de téléphonie, comme le montre l'illustration n°3.

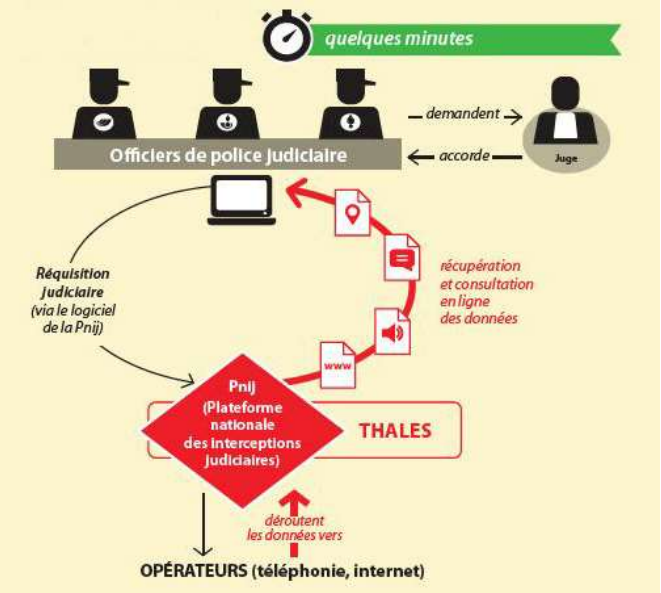


Illustration n°3 : Fonctionnement de la PNIJ[1143]

688. En fait, la qualification précise de cette structure est malaisée car elle n'est, ni une agence, ni un service, mais elle a, pourtant, une existence tangible. D'ailleurs, pour contourner cette difficulté, Mireille IMBERT-QUARETTA[1144], dans son rapport de mai 2017 parle de « mise en œuvre » opérationnelle de la PNIJ[1145]. La PNIJ fait suite à une

[1141] V. **annexe 1, fiche A1/12**.
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. »
V. également l'article 88 de la loi n°2016-731 du 3 juin 2016 *(op. cit.* p.23) qui vient créer l'art. 230-45 dans le C. pr. pén.
[1142] C. pr. pén. art.230-45 : « Sauf impossibilité technique, les réquisitions et demandes […] sont transmises par l'intermédiaire de la plate-forme nationale des interceptions judiciaires qui organise la centralisation de leur exécution. »
[1143] Source : La Dépêche du Midi – 13 octobre 2015.
Thales est l'opérateur qui a obtenu le marché public pour la mise en œuvre opérationnelle de cette plate-forme.
[1144] Contrôleure de la plate-forme nationale des interceptions judiciaires. Cette fonction est prévue par l'art. R40-53 du C. pr. pén.
[1145] IMBERT-QUARETTA Mireille, *1er rapport d'activité, La centralisation des interceptions judiciaires,* mai 2017 : p.11 c'est « l'ANTENJ qui met en œuvre la PNIJ ».

première étape dans le projet de centralisation des écoutes téléphoniques, qui était le système de transmission d'interceptions judiciaires[1146] créé en 2007.

689. Une collecte de données très extensives. – Les données collectées dépassent largement l'enregistrement des conversations téléphoniques, puisque ce sont également les SMS, les MMS, les informations de géolocalisation[1147] et la VOIP qui sont stockés dans la base de données. Toutes les données autres que l'enregistrement des conversations orales sont qualifiées de « prestations annexes ». Celles-ci représentent 99% des réquisitions[1148].

690. Une utilisation des données encadrée. – Toutefois, les possibilités d'investigation sur les données sont très encadrées, afin de préserver les libertés individuelles. Le Code de procédure pénale dispose que « pour les besoins des procédures dont ils sont saisis, les officiers et agents de police judiciaire de la gendarmerie et la police nationales, […] accèdent aux données et informations enregistrées dans le traitement, à l'exception de celles qui sont placées sous scellés[1149] ». On en déduit que les enquêteurs ne peuvent accéder qu'aux données de la procédure et ne peuvent en aucun cas lancer des recherches sur l'intégralité de la base de données de la PNIJ. Ceci est d'ailleurs confirmé par l'autorité compétente de la PNIJ qui affirme « qu'aucun rapprochement n'est possible entre plusieurs dossiers et que le cloisonnement affaire par affaire est une caractéristique technique intrinsèque à la plate-forme[1150] ».

691. Une conservation des données originale et novatrice. – La PNIJ bénéficie d'un régime dérogatoire pour la conservation des données collectées, aussi bien en application de l'interception des correspondances que de la géolocalisation. Alors qu'il est normalement prévu que les données recueillies doivent être placées sous scellés fermés, puis détruits à la fin de la procédure[1151], la PNIJ n'est pas tenue par ces dispositions[1152].

L'ANTENJ a été créée par le 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. Elle remplace la délégation aux interceptions judiciaires.

[1146] Décret n°2007-1145 du 30 juillet 2007 portant création d'un traitement automatisé de données à caractère personnel dénommé « Système de transmission d'interceptions judiciaires ».

[1147] V. *supra* n°509.

[1148] *Ibid.* IMBERT-QUARETTA Mireille, *1er rapport d'activité,* p.12.

[1149] C. pr. pén. art. R40-47.

[1150] IMBERT-QUARETTA Mireille, entretien du 27 septembre 2017 (*op. cit.* p.35).

[1151] V. resp. C. pr. pén. art. 100-4, 100-6, 230-38 et 230-43.

[1152] C. pr. pén. art. 230-45 3ème al.

Cela ne signifie pas que ces données restent directement accessibles aux autorités judiciaires. Il est simplement prévu une procédure technique de mise sous scellés numériques au sein de la PNIJ[1153]. Si un accès aux données se révèle nécessaire ultérieurement, le bris du scellé numérique ne peut être autorisé que par un magistrat et fera l'objet d'une traçabilité complète.

b. Les fichiers de la captation de données

692. Un traitement par procédure. – L'acte de surveillance qu'est la captation des données[1154], possède une correspondance avec des traitements de données à caractère personnel[1155]. Il convient de souligner l'emploi du pluriel, car le raisonnement est le même que pour les interceptions de correspondances, mais avec une mise en œuvre différente. Le principe reste la séparation des données enquête par enquête avec l'interdiction de regrouper des données captées au travers de procédures différentes[1156]. Néanmoins, à la différence de la PNIJ qui a pour vocation de centraliser toutes les écoutes de lignes téléphoniques, la captation de données reste une mesure d'investigation « locale », puisqu'il faut être à proximité[1157] de l'appareil numérique qui est la cible de la mesure.

693. Ainsi, ce sont autant de traitements de données qui sont créés que de mesures de captation de données. Ces traitements ne sont donc pas centralisés dans une base nationale et sont gérés localement au sein du service qui suit l'exécution de la mesure correspondante.

694. Conclusion du sous-paragraphe I : les bases de données judiciaires. – Il existe un nombre important de traitements de données à caractère personnel mis en œuvre par les autorités judiciaires. Tout d'abord, certains fichiers font partie intégrante de l'environnement informatique de travail des enquêteurs au quotidien. Ensuite, d'autres

---

[1153] C. pr. pén. art. R40-49 : « Les données et informations mentionnées aux 1° et 2° de l'article R. 40-46 sont placées sous scellés au sein du traitement jusqu'à expiration du délai de prescription de l'action publique. » V. *infra* n°1028.

[1154] C. pr. pén. art. 706-102-1 et s.

[1155] V. **annexe 1, fiche A1/13.**
Décret n°2015-1700 du 18 décembre 2015 relatif à la mise en œuvre de traitements de données informatiques captées en application de l'article 706-102-1 du code de procédure pénale.

[1156] V. art. 4 du décret du 18 décembre 2015 *(ibid.)*. Les magistrats et les enquêteurs accèdent aux données « des procédures dont ils sont saisis. »

[1157] Même si l'implantation du dispositif permettant la captation des données, à distance au travers d'Internet notamment, est prévue : v. C. pr. pén. art. 706-102-5, 2ème al.

sont très spécialisés sur des typologies criminelles, notamment avec pour objectif d'identifier des individus particulièrement dangereux. Enfin, des traitements de données sont mis en œuvre lors de l'exécution d'actes de surveillance.

695. Comme précédemment expliqué, l'appellation « traitement judicaire », dans les présentes, dépasse les fichiers mis en œuvre par les autorités judiciaires car elle englobe tous les traitements directement accessibles en enquête pénale. Or, plusieurs fichiers à vocation administrative, et non judiciaire, répondent à ce critère et sont susceptibles de fournir des données importantes pour la progression d'une procédure pénale.

II – Les bases de données administratives directement accessibles

696. La bivalence du mot « administratif ». – Les autorités judiciaires ont un accès direct, c'est-à-dire prévu par les textes, aux informations contenues dans des traitements de données administratifs. Ces fichiers, qualifiés « d'administratifs », regroupent des bases de données tenues par une administration *(A)* comme le fichier des cartes grises, et des traitements au service de l'activité de police administrative *(B)*. Ces derniers s'inscrivent dans la politique de l'Etat en matière de maintien de l'ordre de public et de prévention.

A. Les traitements administratifs

☞ *V. annexe 1, fiche A1-14.*

697. L'intérêt des fichiers administratifs en enquête pénale. – Un ensemble de fichiers administratifs ont, avant tout, une utilisation dans la vie quotidienne de tout un chacun comme, par exemple, pour prouver son identité notamment pour accéder à certains lieux à accès contrôlés, ou pour montrer que l'on satisfait à des exigences pour accomplir certaines tâches comme conduire telle ou telle catégorie de véhicule. Pour autant, ces traitements de données ont également une double utilité potentielle en enquête pénale. La première, évidente, est de vérifier l'identité d'une personne, mais la seconde peut, en cas de défaut dans l'inscription dans la base de données, constituer une infraction, comme en cas de conduite sans un permis de conduire valable[1158].

[1158] C. de la route art. L221-2.

698. Ainsi, les fichiers suivants sont fréquemment utilisés par les enquêteurs : le fichier national des immatriculations, le système national de gestion des permis de conduire[1159], le système de gestion des cartes nationales d'identité, ou encore le système de gestion des passeports.

699. Le prolongement administratif des antécédents judiciaires. – De plus, certains fichiers administratifs sont proches des fichiers judiciaires relatifs aux antécédents des individus.

700. L'interdiction de détenir des armes. – Le premier est le « fichier national des interdits d'acquisition et de détention d'armes[1160] » qui recense toutes les personnes qui n'ont pas le droit de détenir une arme ou des munitions, par décision administrative, le plus souvent s'appliquant automatiquement en cas de condamnation pénale[1161].

701. La fausse monnaie. – Une seconde base de données s'intitule le « fichier national du faux monnayage (FNFM) ». Celle-ci trouve sa base légale dans un règlement européen de 2001 dont l'objectif est de protéger l'euro[1162]. Ce traitement de données n'est pas un fichier de condamnation (même si le nom des mis en cause est enregistré) mais il contient des éléments sur toutes les affaires de faux monnayages.

702. Des fichiers à l'intérêt marginal. – Néanmoins, la consultation de ces deux fichiers ne constitue pas une investigation numérique majeure. En effet, seules des informations relatives à des infractions très particulières sont susceptibles d'être extraites.

703. Un nombre important de fichiers dans le Code de la sécurité intérieure. – Un ensemble de fichiers administratifs font l'objet d'un titre entier dans la partie règlementaire du Code de la sécurité intérieure[1163]. Leur contenu est accessible aux autorités judiciaires en enquête pénale, sauf cas particulier comme pour PARAFE[1164],

---

[1159] PELISSIER Pierre, *Circulation routière – Responsabilité pénale et poursuites*, Dalloz, Répertoire de droit pénal et de procédure pénale, mai 2019.

[1160] Décret n°2011-374 du 5 avril 2011 portant création du fichier national des personnes interdites d'acquisition et de détention d'armes (FINIADA).
Décret n°95-589 du 6 mai 1995 relatif à l'application du décret du 18 avril 1939 fixant le régime des matériels de guerre, armes et munitions.
C. séc.int. L312-1 et s.

[1161] C. séc. int. L312-3.

[1162] Règlement (CE) n°1338/2001 du 28 juin 2001 définissant des mesures nécessaires à la protection de l'euro contre le faux monnayage.

[1163] C. séc. int. partie règlementaire - livre II - titre III « Traitements automatisés de données personnelles et enquêtes administratives. »

[1164] C. séc. int. art. R232-6 et s.

dont la finalité est « d'améliorer et de faciliter les contrôles de police aux frontières extérieures », est d'accès réservé aux agents en charge du contrôle aux frontières[1165].

704. Le contrôle administratif des usagers de vols internationaux. – En revanche, dans la catégorie des traitements créés pour le contrôle des passagers entrant sur le territoire, API-PNR France[1166] est potentiellement intéressant[1167] car il est complet et large d'accès, notamment, pour les « directions interrégionales et régionales de la direction centrale de la police judiciaire » ainsi que les « sections de recherches de la gendarmerie nationale » dans le cadre des infractions de criminalité organisée. L'utilisation de cette base de données va donc bien au-delà du terrorisme, sa finalité première. Ce fichier, même s'il est clairement à vocation administrative[1168], à savoir d'assurer la traçabilité des passagers, peut s'avérer intéressant dans des enquêtes, au sein desquelles il est nécessaire, par exemple, d'établir des relations entre des complices qui auraient voyagés sur un même vol.

B. Les traitements de police administrative

☞ *V. annexe 1, fiches A1-15 à A1-19.*

705. Le prolongement d'API-PNR à vocation de police administrative. – Le Système d'Information Schengen (SIS)[1169] incarne le passage des bases de données administratives vers celles dédiées au maintien de l'ordre et à la sécurité publique. En effet, API-PNR[1170] peut servir, par exemple, dans le cadre d'une catastrophe aérienne dont les causes sont accidentelles, tandis que le SIS, même s'il prolonge les objectifs de l'API-PNR, a clairement une vocation judiciaire[1171]. Derrière le SIS, ce sont deux

[1165] « Peuvent seuls avoir accès aux données contenues dans le traitement mentionné à l'article R. 232-6 les agents de la police aux frontières et des douanes, individuellement désignés et spécialement habilités par leur chef de service, pour les besoins des contrôles dont ils sont chargés dans les aéroports, ports maritimes et gares ferroviaires concernés. »
[1166] V. **annexe 1, fiche A1/14 -** C. séc. int. art. R232-12 à R232-18.
[1167] « Potentiellement » car l'efficacité de ce fichier résulte de sa mise en œuvre au niveau Européen et pas uniquement en France. C'est au moment des attentats de Bruxelles en mars 2016 que la question du déploiement de ce traitement de données pour l'ensemble des pays européens est devenue particulièrement prégnante.
[1168] CJUE 30 mai 2006, aff.C-317/04 et C-318-04 « Parlement contre Conseil ». Le PNR concerne la sécurité publique.
[1169] V. **annexe 1, fiche A1/15** – C. séc. int. art. R232-12 et s.
[1170] V. *supra* n°704.
[1171] SCHWENDENER Marc, *Police technique et scientifique*, Dalloz Répertoire de droit pénal et de procédure pénale, février 2019 : « […] personnes disparues ou recherchées dans le cadre de procédures pénales […] certains objets : véhicules, armes à feu, billets de banque répertoriés, documents administratifs (vierges ou non) volés, détournés, égarés, aux fins de saisie ou de preuve dans une procédure pénale. »

traitements de données à caractère personnel qui sont présents[1172]. Leur intérêt en tant qu'investigation numérique réside dans le fait d'obtenir des informations sur des individus qui seraient recherchés dans d'autres pays. Toutefois, avec une vision pragmatique, il apparaît rapidement que ces fichiers ne concernent réellement que des infractions graves telles que le terrorisme, la criminalité organisée avec des réseaux internationaux ou de la traite d'êtres humains, notamment la prostitution.

706. Les fichiers de police administrative. – Plusieurs traitements de données sont créés et gérés par les forces de Police et de Gendarmerie dans le cadre de leur mission de police administrative. Ceux-ci ressemblent fortement au traitement d'antécédents judiciaires[1173], mais ont vocation à enregistrer des données sur des personnes susceptibles de causer des troubles à l'ordre public, ce qui constitue une finalité différente et souvent plus extensive.

707. L'accès à ces traitements dans le cadre des enquêtes pénales est explicitement prévu ce qui, concrètement, n'apporte pas grand-chose puisque c'est le plus souvent le même gendarme ou policier qui manipule ces traitements de données administratifs et qui a conjointement une mission de police judiciaire. Ainsi, même si l'accès officiel permettant d'utiliser les informations extraites de ces fichiers administratifs en enquête pénale apporte une légitimité en tant qu'investigation numérique, un accès officieux serait de toute façon impossible à contrôler.

708. Un fichier pour la Gendarmerie à vocation de support administratif. – L'extraction d'informations du traitement de données à caractère personnel dénommé « gestion des sollicitations et des interventions[1174] » ne présente pas d'intérêt en tant qu'investigation numérique, car ce fichier propre à la gendarmerie comporte, d'une part des noms des personnes que l'on peut requérir et, d'autre part, des données sur les personnes faisant appel à une intervention. Or, si ces personnes ayant fait appel aux gendarmes deviennent des victimes dans une procédure qui serait ouverte, elles seront enregistrées dans le traitement d'antécédents judiciaires. En conséquence, la « gestion des

[1172] N-SIS et Gestion Electronique des Documents (GED).
[1173] V. *supra* n°642.
[1174] C. séc. int. art. R236-31et s.
Décret n°2011-341 du 29 mars 2011 portant création d'un traitement de données à caractère personnel intitulé « gestion des sollicitations et des interventions. »

sollicitations et des interventions » est plus une base de données facilitant le travail administratif des enquêteurs qu'un véritable fichier destiné aux investigations.

709. L'héritage du fichier des renseignements généraux. – Trois bases de données sont associées en raison de l'historique qui les entourent. Leur origine commune trouve en grande partie sa source dans le fichier des renseignements généraux[1175] (FRG). Par la suite, l'évolution de ce fichier a généré les turpitudes médiatiques d'EDVIGE en 2008[1176], avant que ces trois bases de données ne prennent la forme sous laquelle elles perdurent depuis 2013[1177]. Il s'agit du fichier « enquêtes administratives liées à la sécurité publique (EASP)[1178] » et de deux bases de données équivalentes : l'une, nommée « prévention des atteintes à la sécurité publique (PASP)[1179] » est destinée à la Police nationale, tandis que l'autre, « gestion de l'information et prévention des atteintes à la sécurité publique[1180] » est pour la Gendarmerie.

710. Une enquête administrative pour des fonctions et emplois sensibles. – L'objectif de l'EASP est d'inscrire dans ce fichier des personnes appelées à occuper des postes particuliers, le plus souvent en lien avec la sécurité[1181] ou souhaitant obtenir la nationalité française[1182]. Les données enregistrées sont vastes puisque « est également conservé le rapport de l'enquête administrative, contenant les éléments permettant de déterminer si le comportement de la personne concernée n'est pas incompatible avec l'exercice des fonctions ou des missions envisagées, compte tenu de leur nature ».

711. Deux bases de données dédiées à la sécurité publique. – Les deux autres traitements de données offrent des possibilités d'investigations importantes aux

---

[1175] Décret n°91-1051 du 14 octobre 1991 portant application aux fichiers informatisés, manuels ou mécanographiques gérés par les services des renseignements généraux des dispositions de l'article 31 (version antérieure à l'ordonnance du 12 décembre 2018), alinéa 3, de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

[1176] V. *infra* n°969.

[1177] Décret n°2013-1113 du 4 décembre 2013 relatif aux dispositions des livres Ier, II, IV et V de la partie réglementaire du code de la sécurité intérieure (Décrets en Conseil d'Etat et décrets simples).

[1178] V. **annexe 1, fiche A1/16 -** C. séc. int. art. R236-1 et s.
Décret n°2009-1250 du 16 octobre 2009 portant création d'un traitement automatisé de données à caractère personnel relatif aux enquêtes administratives liées à la sécurité publique.

[1179] V. **annexe 1, fiche A1/17 -** C. séc. int. art. R236-11 et s.
Décret n°2009-1249 du 16 octobre 2009 portant création d'un traitement de données à caractère personnel relatif à la prévention des atteintes à la sécurité publique.

[1180] V. **annexe 1, fiche A1/18 -** C. séc. int. art. R236-21 et s.
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.

[1181] C. séc. int. art. L114-1, L114-2 et L211-11-1.

[1182] Loi n°95-73 du 21 janvier 1995 d'orientation et de programmation relative à la sécurité, art. 17-1.

enquêteurs lors d'une procédure pénale[1183], puisque toutes « les personnes dont l'activité individuelle ou collective indique qu'elles peuvent porter atteinte à la sécurité publique », ainsi que des « personnes entretenant ou ayant entretenu des relations directes et non fortuites avec l'intéressé[1184] » peuvent être enregistrées dans ces deux fichiers. L'accès à ces données est relativement ouvert puisque « dans la limite du besoin d'en connaître, tout autre membre d'une unité de la Gendarmerie nationale ou agent d'un service de la Police nationale » peut être destinataire des informations, ce qui inclut sans ambiguïté un officier de police judiciaire dans le cadre d'une enquête dont il aurait la responsabilité.

712. Une très large catégorie de personnes fichées. – L'extraction d'informations depuis ces traitements constitue des investigations numériques potentiellement très efficaces car les données qu'ils contiennent couvrent un éventail de personnes bien plus large encore que le traitement d'antécédents judiciaires[1185] puisque peuvent être fichés ici des individus dont le nom n'est jamais apparu dans la moindre procédure judiciaire. Fort heureusement pour le respect des libertés individuelles, les recherches par mots clés au sein de ces bases de données sont encadrées, puisque sont explicitement prohibées les recherches par le biais d'éléments[1186] relatifs à « des signes physiques particuliers » et, surtout, à « des activités politiques, philosophiques, religieuses ou syndicales ».

713. Des fichiers pour les missions opérationnelles. – Dans la continuité des traitements consacrés aux missions de police administrative, la Gendarmerie nationale dispose de quatre traitements qui lui servent de support dans ses missions opérationnelles de police administrative. Ces quatre traitements sont regroupés sous le nom de Base de Données de Sécurité Publique (BDSP). Il s'agit tout d'abord de la « gestion des évènements d'ampleur (GEA) », qui ne présente aucun intérêt en matière d'investigation numérique puisqu'il ne comporte aucune donnée nominative, de la « gestion des sollicitations et interventions » et de la « gestion de l'information et de prévention des atteintes à la sécurité publique » qui viennent d'être étudiés.

[1183] L'accès aux officiers de police judiciaire est prévu aux art. R239-26 et R236-16 du C. séc. int.
[1184] V. resp. C. séc. int. art. R236-12 et R236-22.
[1185] V. *supra* n°641.
[1186] V. resp. C. séc. int. art. R236-13 et R236-23 : « Il est interdit de sélectionner dans le traitement une catégorie particulière de personnes à partir de ces seules données. »
V. également, BATHO Delphine et BENISTI Jacques-Alain, *sur la mise en œuvre des conclusions de la mission d'information sur les fichiers de police,* (*Op. cit.* p.35), p.57 : « En outre, un garde-fou important a été posé […] : ces éléments ne peuvent en aucun cas faire l'objet d'une recherche aveugle. »

714. La BDSP repose sur un quatrième traitement, à savoir la « sécurisation des interventions et demandes particulières de protection[1187] », qui est un fichier particulièrement complet et dont la consultation, par voie de conséquence, constitue une investigation numérique potentiellement intéressante. Tout comme avec le PASP et la « gestion de l'information et prévention des atteintes à la sécurité publique », les possibilités d'extraction avancées de données[1188] sont interdites[1189]. Toutefois, ce fichier peut s'avérer utile au cours d'une enquête pour obtenir des informations sur la dangerosité d'une personne, le fait qu'elle détienne des armes ou un chien de première catégorie, voire même des données sur ses orientations religieuses ou politiques.

715. Il complète le traitement d'antécédents judiciaires[1190] puisque des données relatives à des individus n'ayant pas été cités dans un dossier judiciaire, mais dont la Gendarmerie estime qu'ils peuvent poser des problèmes à l'ordre public, peuvent y être enregistrées. Le croisement[1191] des informations issues de ce traitement avec le TAJ est susceptible d'apporter une grande efficacité de « fichage » des personnes pour les forces de Gendarmerie.

716. Conclusion du paragraphe §1 : les traitements judiciaires pour la consultation. – Les traitements de données à caractère personnel pour la consultation sont interrogés par le biais de mots clés déterminés. Il s'agit la plupart du temps du nom d'une personne afin de savoir si elle est inscrite dans le fichier ciblé par l'enquêteur et, si tel est le cas, d'obtenir les données associées à son nom. Parfois, certains traitements judiciaires autorisent des éléments de consultation plus étendus, comme par exemple les fichiers des empreintes qui peuvent être interrogés à partir de traces dont on ne sait pas à qui elles appartiennent. Il existe une multitude de traitements pour la consultation, de sorte que la recherche d'éventuelles preuves, par les enquêteurs, dans ce dédale de fichiers, est un travail particulièrement minutieux.

[1187] V. **annexe 1, fiche A1/19** – C. séc. int. art. R236-38 et s.
Décret n°2011-342 du 29 mars 2011 portant création d'un traitement de données à caractère personnel relatif à la sécurisation des interventions et demandes particulières de protection.

[1188] Procéder à des recherches par des mots clés quelconques et permettant ainsi de faire apparaître des noms d'individus présent dans le fichier à partir de ces critères.

[1189] C. séc. int. art. R236-41 : « Il est interdit de sélectionner dans le traitement une catégorie particulière de personnes à partir de ces seules données. »

[1190] V. *supra* n°642.

[1191] Le mot « croisement » ne doit pas être pris au sens de la loi informatique et liberté puisqu'il ne s'agit pas d'un croisement informatique de deux bases de données distinctes au départ, mais plutôt au sens de « complémentarité ».

717. A ces traitements pour la consultation, s'ajoutent des fichiers pour lesquels une exploitation informatique des données qu'ils contiennent est autorisée.

§2. Les traitements judiciaires pour la génération de corrélations

☞ *V. annexe 1, fiches A1-20 et A1-21.*

718. L'exploitation informatique des données contenues dans certains traitements. – Les traitements pour la consultation sont des bases de données dont la finalité est de pouvoir obtenir des renseignements sur une personne, ou d'identifier un individu à partir de traces biologiques. Néanmoins, pour certains fichiers, des recherches au travers de mots clés relatifs au contexte entourant des faits, ou correspondants à des éléments matériels, sont autorisées et ont ainsi potentiellement pour résultats des noms d'individus. Ainsi, à partir d'une recherche dans ces fichiers, non nominative, des personnes peuvent se voir suspectées ou impliquées. Il s'agit d'une étape intermédiaire en matière d'investigation avancée dans les bases de données étatiques, dont l'aboutissement est une exploitation au travers de « moteur » au sens informatique du terme[1192] pour établir automatiquement des corrélations entre différentes informations qu'ils contiennent. Il s'agit des traitements pour la corrélation d'informations.

719. La prise de conscience du besoin de regrouper des données issues de procédures différentes. – Des tueurs en série comme Francis HEAULME, Michel FOURNIRET ou Guy GEORGES, fortement itinérants dans l'accomplissement de leurs crimes, ont démontrés dans les années 80 et 90 la nécessité de pouvoir recouper des informations issues de procédures, initialement distinctes, afin de contribuer à la résolution de ces affaires. Il aura pourtant fallu attendre 2011 pour que les autorités publiques, au travers de la loi connue sous le nom de « LOPPSI 2[1193] », créent les fichiers d'analyse sérielle[1194] et les logiciels de rapprochement judiciaire[1195].

[1192] C'est-à-dire des algorithmes permettant une exploitation « intelligente » des données.
[1193] Loi n°2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure.
[1194] V. annexe 1, fiche A1/21. C. pr. pén art. 230-12 et s. – R40-35 et s.
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 ».
[1195] V. annexe 1, fiche A1/20. C. pr. pén. art. 230-20 et s. – R40-39 et s.
Décret n°2012-687 du 7 mai 2012 relatif à la mise en œuvre de logiciels de rapprochement judiciaire à des fins d'analyse criminelle.

720. Deux outils aux finalités proches. – Ces deux traitements, dont la vocation principale est l'exploitation des données selon des algorithmes permettant d'établir des corrélations entre des informations issues de procédures différentes ou, des données recueillies au sein d'une même procédure mais atteignant un fort degré de complexité[1196]. Ces outils d'investigations numériques sont théoriquement puissants, bien que cette puissance dépende directement du volume de données introduit dans la base, de la qualité de ces données (le vocabulaire utilisé doit, par exemple, être homogène d'une procédure à une autre pour désigner les mêmes éléments) et de leur pertinence[1197]. La finalité de ces deux outils est très proche puisqu'il s'agit de procéder à l'exploitation des données, à tel point que l'on peut se demander l'intérêt qu'il y a eu pour le législateur à séparer ces deux traitements.

721. La difficile compréhension de ces outils en raison du flou les entourant. – Dans le détail, et sous réserve de l'opacité qui entoure ces outils[1198], il semble que les logiciels de rapprochement judiciaire créent des bases de données temporaires pour une procédure donnée, tandis que les fichiers d'analyse sérielle ont vocation à constituer une base nationale avec les faits criminels présentant un caractère sériel. Une grande complexité de compréhension et de lisibilité provient également du fait que, derrière ces deux traitements énoncés par le Code de procédure pénale, se trouvent en vérité plusieurs autres traitements, dument déclarés ou pas, correspondants à des logiciels nommément désignés.

722. Ainsi, dans la catégorie des fichiers d'analyse sérielle, pourtant officialisés par le décret du 22 novembre 2013, s'inscrivent SALVAC (système d'analyse des liens de la violence associée aux crimes) déclaré en 2009[1199], ainsi que AJDRCDS[1200] qui est à l'étude. Dans son premier article, le décret de 2009 explique que la finalité de SALVAC est « de faciliter la constatation des crimes et délits portant atteinte aux personnes et présentant un caractère sériel […] ». Il est confié à une cellule dénommée Office central

[1196] V. *supra* n°634.
[1197] Une collecte de données sans aucun discernement ne rime pas toujours avec efficacité. Par exemple, aux Etats-Unis, la NSA qui pratique depuis très longtemps la collecte tous azimuts des données, a montré l'inefficacité d'une telle pratique au moment des attentats de 2001.
[1198] V. *infra* n°725.
[1199] 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 ».
[1200] « Application judiciaire dédiée à la révélation des crimes et délits en série » qui serait mis en œuvre par la Gendarmerie nationale.

pour la répression des violences aux personnes (OCRVP). Selon les spécialistes de ces outils, SALVAC contenait 9421 dossiers au 1er février 2010[1201].

723. Pour les logiciels de rapprochement judiciaire, la situation est pire encore puisque ce ne sont pas moins de 5 traitements qui sont directement déclarés[1202], alors qu'ils entrent dans la définition de l'article 230-20 du Code de procédure pénale. On y trouve toute la suite logicielle d'analyse criminelle[1203] utilisée par la gendarmerie et Mercure dont la Police nationale se sert pour l'exploitation des données issues des écoutes téléphoniques. ANB, au sein de la suite logicielle d'analyse criminelle, joue un rôle important puisqu'il est utilisé par les gendarmes spécialisés au sein des Sections de Recherche pour créer des graphes mettant en évidence des points en communs entre différents faits et, point souvent déterminant dans les dossiers, une ligne du temps.

724. A ces 5 traitements déclarés, doivent être ajoutés deux fichiers en cours d'expérimentation par la Préfecture de police : CORAIL[1204] et LUPIN[1205] dont la finalité serait de procéder à des rapprochements dans le domaine de la petite et moyenne délinquance.

725. Un flou dès les procédures de création de ces traitements. – Il ressort une grande opacité dans les déclarations qui sont faites autour de ces deux grandes familles de logiciels d'investigation numérique car la description des données collectées est particulièrement floue. En effet, les décrets de création des traitements automatisés correspondants renvoient à un dossier technique de présentation du logiciel (évidemment non annexé au décret) pour la description des données enregistrées et des investigations possibles.

726. Une opacité affectant les libertés individuelles. – Ce manque de transparence constitue un problème majeur pour le respect des libertés individuelles, car il est impossible de pouvoir contester ou demander la rectification de données personnelles stockées puisque l'on n'a aucun moyen de savoir quelles sont les informations collectées.

727. Conclusion du paragraphe §2 : les traitements judiciaires pour la génération de corrélations. – Deux traitements ont été créés pour procéder à de l'exploitation

[1201] BAUER Alain et SOULLEZ Christophe, *Les fichiers de police et de gendarmerie, op. cit.* p.35
[1202] CNIL, fiche « ANACRIM : logiciels de rapprochement judiciaire à des fins d'analyse criminelle ».
[1203] ANACRIM-ARTRT, ANACRIM-ANB, ANACRIM-ING et ANACRIM-IVC.
[1204] Cellule opérationnelle de rapprochement et d'analyse des infractions.
[1205] Logiciel d'uniformisation des procédures d'identification.

informatique d'informations collectées à grande échelle. Les régimes entourant le fonctionnement de ces deux outils sont dissimulés par la complexité qui ressort de la confusion entre les logiciels et les traitements de données, ainsi que par un manque total de transparence avec l'utilisation réelle qui est faite des informations collectées. Bien qu'officiellement déclarés, les fichiers d'analyse sérielle et les logiciels de rapprochement judiciaire sont tout aussi confidentiels que des traitements mis en œuvre par les services de renseignements et protégés par le secret défense[1206].

728. Conclusion du chapitre 2 : les régimes de l'extraction de données depuis les traitements judiciaires. – Les traitements judiciaires sont des traitements de données à caractère personnel pour lesquels un accès direct est prévu au stade de l'enquête pénale. Ils contiennent une richesse d'informations qui dépassent largement les antécédents judiciaires des personnes condamnées ou même, qui ont été suspectées lors d'une procédure pénale. En effet, les victimes, mais également toutes les personnes de l'entourage ou fréquentant un individu surveillé par la police ou la gendarmerie peuvent faire l'objet d'un enregistrement dans un ou plusieurs de ces fichiers. Lorsque les traitements judiciaires permettent d'obtenir des données utiles à une procédure, leurs consultations définissent une deuxième catégorie d'investigations numériques. Cette dernière se distingue des actes intrusifs conduisant à l'obtention de données[1207], car les informations numériques sont déjà connues des autorités judiciaires[1208].

729. Conclusion du titre 2 : le constat de la pluralité des régimes. – Néanmoins, les traitements judiciaires ont en commun avec les actes intrusifs, d'être soumis à une multitude de régimes, aussi bien dans les conditions de leur mise en œuvre que pour leurs effets[1209]. Dans le cas des traitements judiciaires, la consultation repose pour certains fichiers, sur des recherches exclusivement réalisées avec le nom d'une personne, tandis que d'autres sont créés pour procéder à des corrélations entre les informations enregistrées. Sur cette distinction, plusieurs traitements révèlent une incohérence entre ce

[1206] V. *supra* n°613.
[1207] Qui sont la première catégorie d'investigations numériques, v. *supra* n°235.
[1208] V. *supra* n°75.
[1209] Dans le cas des traitements judiciaires, les effets sont des consultations des informations stockées. Pour les actes intrusifs, les effets sont une fouille des données ou la génération de données par des outils de surveillance.

que prévoient les dispositions encadrant leur régime de consultation, et la réelle exploitation qui est faite des données[1210].

730. Dans le cas des actes intrusifs permettant l'obtention de données, la pluralité des régimes a plusieurs causes. En premier lieu, les investigations numériques intrusives sont placées sous des régimes très différents dans leur condition de mise en œuvre. Pour celles faisant partie de la procédure de droit commun[1211], certaines peuvent être utilisées par les enquêteurs pour toutes les infractions, tandis que d'autres sont réservées à des infractions punies d'un certain seuil d'emprisonnement[1212]. Dans le cas des actes de surveillance, un double régime se cumule en ajoutant à l'autorisation de mise en œuvre de l'acte lui-même, une autorisation distincte pour la mise en place du dispositif technique nécessaire aux opérations. Cette multitude de régimes différents se retrouvent lors de l'exécution de l'acte où les opérations d'analyse des données sont parfois, très encadrées comme dans le cas de l'exploitation des scellés saisis lors d'une perquisition, alors que pour des mesures comme le déchiffrement des données, leur analyse n'est même pas explicitement prévue. En second lieu, la pluralité des régimes résulte directement de l'éparpillement des actes d'investigations numériques au sein du Code de procédure pénale.

731. Conclusion de la première partie : le constat de l'éparpillement des investigations numériques. – Les investigations numériques intrusives sont présentes aussi bien dans la procédure de droit commun que dans les procédures dérogatoires, tout particulièrement celle applicable à la criminalité et à la délinquance organisées. Cette dernière contient beaucoup d'investigations numériques, comme les IMSI-catcher ou la captation des données. Elle prévoit également l'extension d'un acte issu de la procédure de droit commun, les écoutes téléphoniques, au stade de l'enquête.

Dans le cas des investigations numériques que sont les extractions de données depuis les traitements judiciaires, la situation est pire encore car les dispositions encadrant ces traitements sont souvent le fait de décrets non codifiés, voire de simples arrêtés[1213]. Cet éparpillement, dont découle pour partie la multitude des régimes applicables, induit une

[1210] Par ex. v. *supra* n°647.

[1211] Ex. : les écoutes téléphoniques (v. *supra* n°293.) ou la fouille des scellés numériques (v. *supra* n°528.).

[1212] Ex. : la géolocalisation (v. *supra* n°489.).

[1213] V. par ex. le traitement automatisé de contrôle des données signalétiques des véhicules, créé par l'arrêté du 18 mai 2009 ainsi que tous les traitements mis en œuvre pour la constatation des infractions au Code de la route.

importante hétérogénéité des investigations numériques, les rendant illisibles pour la plupart des praticiens du droit.

732. Néanmoins, cette situation ne concerne pas que les investigations numériques. Elle est constatée pour l'ensemble de la procédure pénale. Lors de la promulgation de la loi du 23 mars 2019, certains auteurs n'ont pas hésité à parler « d'une procédure qui devient, à chaque réforme, de plus en plus immaîtrisable[1214] ». Ainsi, l'illisibilité des investigations numériques n'est que le reflet de la procédure pénale dans son ensemble. La présente étude n'a pas vocation à proposer une réforme globale de la procédure pour réduire cette complexité[1215]. La première partie de cette étude a pour objectif d'étudier tous les actes permettant d'obtenir des données au sein d'une enquête, malgré la complexité globale dans laquelle ils s'inscrivent.

733. Dans un second temps, c'est en raisonnant sur les données obtenues au terme de chaque investigation numérique, que des améliorations importantes peuvent être proposées. Ces dernières peuvent contribuer à améliorer, aussi bien l'efficacité de l'enquête, que la protection des libertés individuelles.

[1214] VERGES Etienne, *Réforme de la procédure pénale : une loi fleuve, pour une justice au gré des courants. A propos de la loi n°2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice,* LexisNexis, Droit pénal n°5, mai 2019, étude 12.

[1215] De nombreuses études sont dédiés à la transformation de la procédure pénale : v. par ex. :
TOUILLIER Marc, *Procédure pénale de droit commun et procédures pénales spéciales,* Thèse soutenue le 30 nov. 2012 à Montpellier 1.
POTASZKIN Tatiana, *L'éclatement de la procédure pénale : vers un nouvel ordre procédural pénal ?*, Thèse soutenue en 2009 à Toulouse1 Capitole.
AYADI Rim, *Théorie pour la réforme de la procédure pénale : éléments pour une définition juridique de la réforme*, Thèse soutenue le 12 décembre 2011 à Montpellier 1.

SECONDE PARTIE.
LA NECESSITE DE REGROUPER LES DONNEES DES INVESTIGATIONS NUMERIQUES

734. Un arsenal particulièrement puissant. – La recherche des preuves en procédure pénale s'est bien adaptée à la numérisation de notre société[1216]. Les investigations numériques sont le fruit de cette adaptation. Elles offrent aux enquêteurs une puissance d'investigation potentiellement redoutable.

735. Le cloisonnement néfaste des données. – Néanmoins, malgré cette puissance incontestable, les investigations numériques pourraient être améliorées. En effet, elles sont des actes de procédure qui ont pour effet d'obtenir des données[1217]. Or, ces dernières sont fortement cloisonnées, ce qui peut être un frein important à l'efficacité de l'enquête, ou ce qui peut nuire au respect des libertés individuelles.

736. La nécessité de regrouper les données. – Le cloisonnement signifie que les différentes données issues ou manipulées lors d'une investigation numérique ne peuvent pas être exploitées ensemble. La présente étude a pour objectif de démontrer les effets

[1216] V. *supra* n°16.
[1217] V. *supra* n°191.

positifs qu'apporterait la consolidation[1218] des données aux investigations numériques dont elles proviennent, et donc à l'enquête et à la procédure pénale.

737. La nécessité de distinguer les deux catégories d'investigations numériques. – Les causes du cloisonnement des données ainsi que, par voie de conséquence, les solutions proposées dans la présente étude, sont différentes suivant qu'il s'agit des investigations numériques intrusives[1219] *(Titre I)* ou exploitant les informations contenues dans les traitements judiciaires[1220] *(Titre II)*.

[1218] Le mot « consolider » doit être entendu au sens comptable, puisque l'objectif est de regrouper ces données pour en améliorer l'exploitation.
Larousse : « pratique comptable qui consiste à agréger les comptes des sociétés [..] en vue de présenter […] la situation financière d'ensemble. »
[1219] V. *supra* n°235.
[1220] V. *supra* n°603. - Sur la notion de traitements judiciaires, v. *supra* n°609.

TITRE I. LA NECESSITE DE REGROUPER LES DONNEES OBTENUES PAR LES ACTES INTRUSIFS

738. Le constat du cloisonnement des données. – Les actes intrusifs permettant l'obtention de données constituent une première catégorie d'investigations numériques[1221]. Or, les données obtenues sont cloisonnées, c'est-à-dire qu'elles sont isolées les unes par rapport aux autres. Par exemple, les données d'un disque dur placé sous scellés sont analysées lors de l'exécution d'un acte[1222], tandis que les données issues d'une captation des données[1223] sont exploitées distinctement. A aucun moment, la procédure actuelle ne prévoit que les données issues de ces deux mesures, puissent être regroupées et analysées ensemble au sein d'un même acte.

739. L'apport potentiel des techniques des données de masse. – Or, l'exploitation des données consolidées serait potentiellement beaucoup plus efficace que l'analyse séparée des informations numériques, grâce aux techniques d'analyse des données de masse (le *big data*[1224]) qui sont actuellement en plein développement.

[1221] V. *supra* n°235.
[1222] V. *supra* n°293.
[1223] V. *supra* n°570.
[1224] V. *infra* n°766.

740. L'enjeu de l'analyse regroupée de toutes les données recueillies lors des différentes investigations. – L'un des enjeux de la présente étude consiste à proposer l'amélioration de l'efficacité de l'enquête pénale en levant les verrous qui empêchent l'exploitation conjointe des données issues de plusieurs actes, notamment celles générées ou recueillies lors de mesures antérieurement exécutées et terminées.

741. Pour parvenir à ces propositions, il est nécessaire de définir le cloisonnement des données et en quoi celui-ci nuit concrètement à l'efficacité de l'enquête *(Chapitre 1)*, afin d'être en mesure d'énoncer les améliorations correspondantes *(Chapitre 2)*.

Chapitre 1. L'efficacité des investigations numériques entravée par le cloisonnement des données

742. Des données cloisonnées par l'acte qui a conduit à les obtenir. – Une investigation numérique est un acte de procédure qui a pour effet de générer ou de recueillir des données. A ce titre, les données obtenues lors de l'exécution d'un acte intrusif[1225] sont liées à celui-ci. Ce lien, très fort, a pour effet de cloisonner les données, c'est-à-dire de les enfermer au sein de la mesure qui a conduit à les obtenir.

743. L'exploitation des données entravée par le cloisonnement. – Or, ce cloisonnement nuit potentiellement à l'efficacité de l'exploitation des données. En effet, cet enfermement des données a pour conséquence de rompre la continuité des informations numériques obtenues au cours d'une enquête *(Section 1)*.

De plus, le cloisonnement des données est amplifié lorsque les différentes investigations numériques, qui sont exécutées au cours d'une procédure, sont confiées à des intervenants différents *(Section 2)*.

Section 1. La rupture de la continuité numérique

744. Les objectifs généraux de la dématérialisation. – Lorsqu'il est question de dématérialisation dans un domaine d'activité quel qu'il soit, la numérisation d'un processus[1226] ou la création d'un système d'information au sein d'un organisme, poursuit invariablement deux objectifs : l'amélioration de la productivité des utilisateurs notamment grâce à une plus grande vitesse dans l'échange et la transmission des informations, et une consolidation des données pour en augmenter le potentiel d'exploitation. D'autres objectifs peuvent être recherchés en fonction de besoins plus spécifiques à un domaine d'activité comme l'amélioration de l'efficacité[1227] ou de la qualité[1228].

[1225] V. *supra* n°235.

[1226] Larousse : « Suite continue d'opérations, d'actions constituant la manière de faire, de fabriquer quelque chose. »

[1227] C'est le cas en procédure pénale où les investigations numériques fournissent des outils d'enquête plus puissants.

[1228] Comme dans le domaine aéronautique où la recherche du zéro défaut est une priorité absolue. L'informatique va notamment permettre d'augmenter la précision et la traçabilité des tests.

745. L'amélioration de l'efficacité. – La procédure pénale n'échappe pas à cette règle puisque la performance des enquêteurs s'est accrue grâce aux investigations numériques. Par exemple, une filature mobilise moins d'effectif en utilisant la géolocalisation en temps réel[1229] ou encore les écoutes téléphoniques[1230] avec la PNIJ[1231] qui produisent des enregistrements audio numérisés avec un accès centralisé. L'utilisation du dispositif est beaucoup plus efficace que les anciennes bandes magnétiques. Néanmoins, cette augmentation de la performance doit être nuancée car les nouvelles technologies ont, certes, amélioré la productivité des enquêteurs sur certaines tâches existantes, mais elles en ont également créé de nouvelles qui n'existaient pas auparavant[1232].

746. L'amélioration inachevée de l'efficacité de l'enquête. – Même si l'apport des outils numériques améliore l'efficacité de l'enquête pénale, le cloisonnement des données, acte par acte, bride considérablement l'exploitation des informations numériques en rompant la continuité de celles-ci *(§1)* ce qui se répercute sur le potentiel d'analyse des données *(§2)*.

§1. Le manque de continuité numérique de l'information

747. L'incompatibilité de la séparation des actes avec la continuité de l'information numérique. – Les outils informatiques sont un support à la dématérialisation des informations. Ils apportent une puissance de traitement grâce, notamment, à un enrichissement permanent des données *(I)*. Malheureusement, en procédure pénale, ce potentiel d'enrichissement se heurte à plusieurs difficultés *(II)*.

I – L'enrichissement de l'information par la continuité numérique

748. La notion de données « riches ». – L'un des principaux intérêts de la dématérialisation d'un « processus métier[1233] » est de manipuler des données numériques « riches ». On entend par « riches » des données informatiquement intelligibles[1234], dont on peut exploiter le contenu. De même, on qualifie souvent de « riche », une information numérique qui contient des métadonnées[1235]. L'exemple le plus concret est celui d'un

[1229] V. *supra* n°489.
[1230] V. *supra* n°528.
[1231] V. *supra* n°687.
[1232] Par ex. l'analyse de supports numériques, la captation de données, etc.
[1233] V. *supra* n°744.
[1234] Par opposition, par exemple, à un document scanné en format image. V. *infra* n°751.
[1235] Une métadonnée est une donnée servant à définir ou décrire une autre donnée.

fichier image, pour lequel les métadonnées, non visibles dans l'image elle-même, indiquent l'heure à laquelle a été pris le cliché, avec quel appareil ou encore avec quels réglages[1236].

749. Ces données « riches », prises dans leur ensemble, sont parfaitement adaptées aux recherches avancées réalisées lors de l'analyse d'un support numérique les contenant. Ce sont, notamment, les recherches par mots clés, qui exploitent fréquemment les métadonnées. Plus généralement, les données riches permettent toute sorte d'exploitation visant à leur donner de l'intelligence ou du sens, en offrant notamment des possibilités d'extractions statistiques[1237]. En matière pénale, pour reprendre une expression familière souvent employée par les enquêteurs, on pourra dire qu'il s'agit de « faire parler » des données.

750. La notion de chaîne numérique. – Dans un système d'information, il se crée donc naturellement une sorte de « chaîne numérique », au cours de laquelle une information s'enrichit à chaque fois qu'elle est exploitée et complétée par un interlocuteur différent ou lors d'une nouvelle étape d'un processus.

751. La rupture de la chaîne numérique. – Or, le danger pour la performance de l'exploitation des données est que cette chaîne numérique soit interrompue, notamment, par le papier. Typiquement, il peut s'agir d'une étape où une signature manuscrite est exigée pour valider un document, car aucune procédure de validation numérique[1238] n'a été mise en place. Il faut donc imprimer ce document.

752. Même si ce document est scanné puis réintroduit dans le système d'information, il a perdu la quasi-totalité de son intérêt numérique puisqu'il ne devient qu'une image, empêchant ainsi son indexation[1239] et les recherches performantes par mots clés sur son contenu. Les logiciels de reconnaissance de caractères[1240] tentent de pallier cette difficulté, mais le résultat n'est généralement que partiel, voire même impossible si le document en question est entièrement manuscrit[1241].

[1236] Ce sont les données EXIF : « *Exchangeable image file format* ». Il s'agit d'un format de fichier normalisé pour définir les métadonnées qui accompagnent l'image elle-même.

[1237] Par exemple, en comptabilité analytique, l'exploitation de données permet de déterminer des rentabilités, des évolutions fines d'une activité industrielle ou commerciale, etc.

[1238] Par le biais d'une signature numérique telle que prévue par l'art. 1367 du C. civ.

[1239] Processus informatique qui consiste à indexer un fichier, c'est-à-dire à le référencer lui, ainsi que tout ce qu'il contient, dans une base de données.

[1240] Appelés logiciels OCR comme « *Optical Character Recognition* ».

[1241] Exemple : un soit-transmis sur lequel le magistrat écrit des consignes à la main pour les officiers de police judiciaire.

753. Conclusion du sous-paragraphe I : l'enrichissement de l'information par la continuité numérique. – L'efficacité de la dématérialisation repose sur une continuité de l'information sous sa forme numérique. Cette sorte de chaîne numérique est essentielle pour la performance de l'exploitation des informations dématérialisées. En effet, à chaque étape, des données s'ajoutent, rendant ainsi l'information de plus en plus riche.
Or, en procédure pénale, plusieurs obstacles empêchent la continuité numérique des informations.

II – Les obstacles à la continuité numérique

754. L'obstacle causé par la résistance du papier. – En procédure pénale, même si celle-ci commence à se dématérialiser[1242], une forte culture du papier subsiste. Par exemple, il ne sert à rien, pour un expert, d'envoyer son rapport d'expertise en version *pdf* puisque le greffier doit l'imprimer pour coter chaque page, puis scanner celui-ci pour que le numéro des cotes apparaisse. D'ailleurs, des travaux sur ce sujet expliquent que « le règne du papier résiste [et que] la transition vers l'immatériel n'est encore qu'à ses balbutiements[1243] ». Comme précédemment expliqué, ce passage par le papier contribue à nuire à l'enrichissement des informations numériques[1244] puisqu'un rapport d'expert ou un procès-verbal rédigé par les enquêteurs, pourrait être indexé[1245] et, ainsi, apporter plus de données potentiellement exploitables lors d'un acte ultérieur.

755. L'obstacle causé par la séparation des actes. – Outre la résistance du papier, le principal obstacle à la continuité numérique des informations au sein d'une enquête trouve sa source dans le principe de séparation des actes en procédure pénale. Cette séparation n'est pas explicitement énoncée dans le Code de procédure pénale et elle est tellement évidente pour la doctrine qu'aucun auteur ne la définit. Ce principe puise son origine dans deux dispositions qui constituent le fondement de la recherche de la vérité que sont les articles 41 et 81 du Code[1246]. Le procureur ou le juge d'instruction procèdent à « tous » les actes nécessaires. Par suite, l'ensemble du Code définit des actes au régime

[1242] V. *supra* n°42.
[1243] *Op. cit.* p.20. TOURE Aminata, *L'influence des nouvelles technologies dans l'administration de la justice pénale.* P. 146.
[1244] V. *supra* n°751.
[1245] V. *supra* n°752.
[1246] C. pr. pén. art. 41 : « Le procureur de la République procède ou fait procéder à tous les actes nécessaires à la recherche et à la poursuite des infractions à la loi pénale. […] »
C. pr. pén. art. 81 : « Le juge d'instruction procède, conformément à la loi, à tous les actes d'information qu'il juge utiles à la manifestation de la vérité. […] »

très différent, tant dans la mise en œuvre que dans les effets. La séparation des actes les uns par rapport aux autres découle de cette structuration de la procédure pénale.

756. Or, cette séparation crée une quasi-autonomie dans l'exécution des actes, les uns par rapports aux autres. L'un des principaux intérêts de cette séparation est de limiter les effets de propagation de l'annulation d'un acte à d'autres actes ou d'autres procédures[1247]. La séparation ne signifie évidemment pas qu'il n'existe aucun lien entre les différents actes. Par exemple, une mesure est souvent ordonnée en fonction du résultat de l'exécution d'un acte précédent. Une perquisition peut être décidée à la suite du résultat d'une écoute téléphonique qui a aiguillé les enquêteurs vers le propriétaire du lieu perquisitionné.

757. Néanmoins, malgré ce lien, un acte a, un début[1248], une durée de vie qui, en matière d'investigation numérique comporte l'obtention de données, et une fin avec la rédaction du procès-verbal[1249] ou du rapport précédemment évoqué qui est versé à la procédure.

758. La mise sous scellés des données comme conséquence de la séparation des actes. – Or, lorsque l'investigation numérique se termine, les enquêteurs ou l'expert, mettent les données sous scellés, conjointement à la remise du rapport ou du procès-verbal. Pour la majorité des investigations numériques, cette mise sous scellés est obligatoire et dument prévue par la loi[1250] ou le règlement[1251].

759. Le cloisonnement des données comme conséquence de la mise sous scellés. – Cette mise sous scellés intervenant lorsque l'acte se termine induit un cloisonnement des informations au sein des différentes investigations numériques diligentées au cours d'une enquête. En effet, le seul lien qu'autorise la procédure pénale entre les actes repose sur le rapport ou le procès-verbal précédemment remis[1252].

[1247] Sur les effets de l'annulation d'un acte v. *infra* n°870.

[1248] Ordonnance d'un juge d'instruction, décision d'un officier de police judiciaire en réaction à une situation comme en enquête de flagrance, mesure jugée utile par l'OPJ au sein d'une commission rogatoire, etc.

[1249] PRADEL Jean, *Procédure pénale*, 19ème édition, Cujas, p.729 : « Ces actes doivent donner lieu à un procès-verbal, seul moyen d'en assurer la conservation. »

[1250] V. par ex. les investigations numériques au sein des techniques spéciales d'enquête prévues au sein de la procédure applicable à la criminalité et à la délinquance organisées et aux crimes (v. *supra* n°448.) , C. pr. pén. art. 706-95.18 : « […] Les enregistrements sont placés sous scellés fermés. […] »). V. eg. la géolocalisation, C. pr. pén. art. 230-38 : « […] Les enregistrements sont placés sous scellés fermés. »), etc.

[1251] Dans le cas de la PNIJ, ce sont sous « scellés [numériques] au sein du traitement » que doivent être placées l'ensemble des informations collectées (C. pr. pén. art. R40-49).

[1252] V. *supra* n°757.

760. Conclusion du paragraphe §1 : le manque de continuité numérique de l'information. – Les investigations numériques sont des actes d'enquête permettant l'obtention de données. La conception de la procédure pénale repose sur un principe de séparation des actes les uns par rapport aux autres. Par voie de conséquence, les données obtenues au sein d'une mesure deviennent inaccessibles lors de l'exécution d'actes ultérieurs, ce qui tronque le potentiel d'analyse de ces données.

§2. L'analyse tronquée des données

761. Le fonctionnement des logiciels *forensiques*. – Pour comprendre en quoi le cloisonnement des données nuit à l'efficacité potentielle des analyses qui peuvent être réalisées, il est nécessaire de décrire le fonctionnement des logiciels d'analyse *forensique* qui sont utilisés pour procéder à l'exploitation des supports numériques[1253], aussi bien par les experts que par les enquêteurs spécialisés en technologies numériques[1254]. Ces logiciels ont plusieurs fonctionnalités. Ils permettent, notamment, de retrouver des données supprimées ou endommagées[1255], de s'affranchir des mots de passe d'ouverture de session pour accéder aux données d'un utilisateur, de trier les données par catégories ou de regrouper les images[1256].

762. L'exploitation des données en quantité très importante. – De plus, l'une des fonctionnalités offrant l'efficacité le plus importante aux enquêteurs, repose sur l'indexation[1257] et le traitement de toutes les données présentes sur un support numérique. Depuis l'avènement de l'informatique personnelle, les supports numériques quels qu'ils soient[1258], ont vu leur capacité décuplée permettant de stocker un nombre de fichiers de plus en plus important. A ces informations créés ou stockées par les utilisateurs, s'ajoutent les données du système d'exploitation de l'appareil, qui sont souvent déterminantes pour les enquêteurs[1259]. On comprend alors qu'il n'est pas réaliste, pour le technicien procédant

[1253] V. *supra* n°293.
[1254] V. *supra* n°323.
[1255] Selon différents niveaux de recherche : des fichiers considérés comme effacés par le système d'exploitation, en reconstruisant des morceaux de fichiers présents dans les espaces libres du disque dur : v. *supra* n°10.
[1256] Cette fonctionnalité est précieuse dans des dossiers de pédopornographie.
[1257] V. *supra* n°752.
[1258] Disque dur d'ordinateur, clé USB, mémoire interne des téléphones portables, carte mémoire, etc.
[1259] Par ex. les caches des navigateurs Internet, mais aussi les bases de registre qui gardent en mémoire tous les périphériques de stockage qui sont connectés à un ordinateur, tous les fichiers temporaires liés à l'utilisation d'un logiciel, des données systèmes montrant la fréquence d'utilisation de certaines applications, etc.

à l'analyse du support, de parcourir tous les fichiers contenus dans plusieurs téra octets de données dans l'espoir de trouver des éléments en rapport avec les faits, d'autant plus que, souvent, ces fichiers ne sont pertinents que lorsque les informations qu'ils contiennent sont recoupées et associées entre elles. C'est là que l'indexation et le travail sur les données que réalise le logiciel d'investigation prennent toute leur importance en permettant, notamment, des recherches par mots clés très avancées[1260]. C'est lors de cette étape que le technicien peut recouper des données afin de leur donner un sens en rapport avec les faits du dossier.

763. De plus, l'indexation présente un autre intérêt. En effet, les logiciels d'investigations disposent, dans la majorité des cas, de bases de données préconstituées. Certaines, sont mondiales[1261], et d'autres peuvent être créées spécialement pour certaines recherches[1262]. Lors de l'étape d'indexation, les données présentes sur le support numérique sont comparées à ces bases de données préconstituées et l'attention de la personne procédant à l'analyse est donc automatiquement attirée.

764. La performance de l'analyse des données regroupées. – Dans le contexte d'une immensité d'informations numériques à exploiter, on en déduit que l'analyse d'une quantité de données « A » qui seraient issues d'une première investigation, et l'analyse de données « B » issues d'une autre investigation risquent de ne pas être aussi performantes que l'analyse des données de « A + B ». Par exemple, un simple nom présent dans un smartphone peut ne pas attirer l'attention de l'enquêteur procédant à l'analyse, alors qu'associé aux données issues d'un disque dur, la même analyse peut révéler des indices aiguillant les enquêteurs dans une nouvelle voie. Ce besoin d'analyser les données regroupées ne peut que s'accentuer dans l'avenir, principalement pour deux raisons.

765. La nécessité de regrouper les données pour lutter contre les techniques de dissimulation – En premier lieu, les délinquants et les criminels ont conscience que leur téléphone, leur ordinateur ou leur messagerie électronique peuvent contenir des

[1260] Avec des caractères génériques, sur des formats de données (par ex : des numéros de téléphone, des numéros de carte bancaire, etc).
[1261] Comme en matière d'images pédopornographiques ou de documents issus de mouvements terroristes.
[1262] Ces bases de données fonctionnent avec la signature numérique des fichiers. Il ne faut pas confondre cette notion de signature numérique avec celle à laquelle l'article 1367 du Code civil fait référence. Ici, on entend par signature (ou empreinte) numérique, une suite binaire de données qui permet de reconnaître le fichier.

informations que les enquêteurs sont susceptibles d'exploiter s'ils sont suspectés. Ils utilisent donc tous les moyens mis à leur disposition pour se protéger, notamment en cryptant les données[1263]. Or, les quelques informations qui peuvent avoir échappé à la vigilance de ces personnes[1264], tels que des traces de fichiers ou de pages *web* qui restent dans des caches du système d'exploitation, et recueillies sur différents appareils, doivent être analysées de manière regroupée pour offrir la meilleure efficacité possible.

766. La nécessité de regrouper les données pour bénéficier de l'évolution des techniques informatiques – En second lieu, la recherche informatique concentre actuellement beaucoup d'effort sur le *big data.* Si l'on s'en tient à une traduction basique, le *big data* se réfère à l'exploitation des données de masse[1265] comme en matière d'épidémiologie[1266] ou de reconnaissance faciale.

767. Dans le cas des investigations numériques, prises à l'échelle d'une procédure, on ne peut évidemment pas parler de données de masse, à l'exception des fichiers d'analyse sérielle[1267]. Dans ce cas précis, une base de données nationale est créée et permet des recherches avancées[1268] sur les informations stockées de manière transversale à toutes les procédures dont sont issues les données. Hormis ce cas particulier, les données recueillies ou générées au sein d'une procédure ne représentent pas à proprement parler des *big data*, mais peuvent pour autant bénéficier des progrès apportés par cette discipline. En effet, les chercheurs travaillent dans ce domaine à créer de nouveaux outils visant notamment à offrir des possibilités d'analyses intelligentes[1269], prédictives[1270] et donc, par voie de conséquence, de plus en plus performantes dans l'interprétation des données. Par exemple, dans une affaire criminelle à San José aux Etats Unis, c'est l'exploitation conjointe des données générées par un bracelet *Fitbit*[1271] avec les données extraites d'un

[1263] Il est facile de trouver sur Internet des logiciels gratuits qui vont permettre de crypter des dossiers sur un support numérique, ou une clé USB, etc. Ex. : VeraCrypt.
[1264] Soit par négligence, soit par mauvaise utilisation des outils de cryptage.
[1265] Kambatla, Karthik and Kollias, Giorgos and Kumar, Vipin and Grama, Ananth, *Trends in big data analytics*, Journal of Parallel and Distributed Computing, pages 2561-2573, 2014, Elsevier.
BERGE Jean-Sylvestre et LE METAYER Daniel, *Données - Phénomènes de masse et droit des données,* LexisNexis, Communication commerce électronique, décembre 2018.
[1266] Wallianallur Raghupathi and Viju Raghupathi, *Big data analytics in healthcare : promise and potential*, Health Information science and systems, 2014.
[1267] V. *supra* n°719. Annexe1, fiche A1/21.
[1268] V. *supra* n°634.
[1269] La recherche en informatique parle de *deep learning* ce qui rejoint l'intelligence artificielle. VILLANI Cédric, *rapport de synthèse france intelligence artificielle,* 28 mars 2018.
[1270] LENA Maud, *Les rapprochements judiciaires*, Dalloz AJ pénal 2017 p.305 : « De nouveaux outils d'analyse prédictive sont maintenant utilisés. Ils permettent de fournir des données opérationnelles […] »
[1271] « Montre » qui mesure l'activité physique de la personne qui la porte : www.fitbit.com

système de vidéoprotection qui a permis d'identifier le meurtrier[1272]. Un rapprochement manuel d'une telle quantité d'informations est impossible.

768. Les logiciels *forensiques* constituent un terrain de prédilection pour la mise en œuvre pratique de l'ensemble de ces techniques, puisque « faire parler » des données est quasiment impossible si l'enquêteur tente de les analyser en les parcourant avec un simple « explorateur de fichier ». Leur évolution dans les années à venir, grâce aux techniques issues du *big data*, améliorera l'assistance à l'enquêteur au travers des corrélations avancées que les logiciels auront la capacité de produire lors de l'analyse. En effet, les données personnelles générées par une personne sont représentatives de sa façon de se comporter, de ses goûts et de ses habitudes, sans oublier qu'elles permettent le plus souvent de tracer son parcours quotidien à la fois professionnel et personnel. Si, en enquête pénale, on y ajoute les données obtenues auprès de tiers[1273], mais qui concernent la personne ciblée par une enquête, on comprend en quoi il est important de pouvoir procéder aux recoupements de toutes les données.

769. Conclusion de la section 1 : la rupture de la continuité numérique. – Le cloisonnement des données acte par acte empêche la continuité numérique des informations au sein d'une enquête. En effet, les échanges d'informations au sein de la procédure sont réalisés au travers de rapports et de procès-verbaux. Les données exploitées lors de chaque investigation sont mises sous scellés au moment où ce rapport ou ce procès-verbal est versé au dossier, ce qui est à l'origine du cloisonnement des données. La continuité numérique offrirait pourtant une meilleure efficacité dans l'exploitation des données obtenues au travers des actes intrusifs. En effet, les logiciels *forensiques* permettent d'établir des corrélations entre des données qui ne sont possibles que si celles-ci sont regroupées et analysées ensemble.

770. De plus, l'enfermement des informations numériques au sein de l'acte ayant conduit à leur obtention est accentué par la dispersion des données à exploiter auprès d'intervenants différents.

[1272] 01NET, *Un traqueur d'activité balance un meurtrier*, 01net n°918, 20 octobre 2019.
[1273] V. *supra* n°372.

Section 2. La dissémination des données auprès d'intervenants différents

771. L'amplification de la rupture de la continuité numérique par la dissémination des investigations. – La rupture de la continuité numérique des données obtenues au travers des actes intrusifs[1274] est amplifiée par la dissémination des investigations. En effet, lorsque plusieurs actes mettant en œuvre des investigations numériques sont ordonnés, il est fréquent que ces différentes mesures soient confiées à des intervenants différents[1275]. Par voie de conséquence, non seulement les données exploitées au sein de ces actes se retrouvent cloisonnées en raison de la rupture de la continuité numérique mais, cumulativement, elles sont souvent disséminées auprès de multiples intervenants *(§2)*, ce qui va à l'encontre du savoir qu'il est nécessaire d'acquérir pour conduire avec efficacité une enquête *(§1)*.

§ 1. - L'importance du savoir dans l'enquête

772. Le rôle central du directeur d'enquête. – Lorsqu'une entité[1276] enquête, cela revient concrètement à confier à une personne, le directeur d'enquête, la responsabilité de procéder aux recherches conduisant à la manifestation de la vérité. Bien évidemment, ce directeur d'enquête travaille avec une équipe, dont les membres accomplissent un certain nombre d'actes[1277].

773. La nécessité de maîtriser l'intégralité du dossier. – Outre le fait de centraliser les informations et la conduite du dossier, y compris lorsque ce pouvoir lui a été délégué par un magistrat[1278], cette gestion centralisée par le directeur d'enquête a surtout pour bénéfice de générer un pilotage homogène, une coordination avec une sorte de savoir qui se crée spécifiquement pour le dossier. C'est ainsi que dans le cas de crimes en série ou dans le cas de disparitions d'enfants nécessitant un travail hautement minutieux dans la

[1274] V. *supra* n°235.
[1275] Enquêteur différent (d'un laboratoire de police, etc), expert judiciaire (v. *supra* n°301.).
[1276] De la Gendarmerie, de la Police ou, plus rarement, des Douanes.
[1277] Audition, transport sur les lieux, suivi du déroulement d'une garde à vue, etc.
[1278] Le parquet au stade de l'enquête préliminaire et le juge d'instruction par commission rogatoire.

collecte et l'exploitation des moindres informations susceptibles de faire avancer le dossier, des cellules dédiées sont créées[1279].

774. En effet, le travail d'enquête est un travail pointu, souvent fondé sur des intuitions ou des soupçons[1280] qui sont éventuellement corroborées au fur et à mesure que le processus avance. Ainsi, il est évident que ces intuitions ou ces soupçons ne sont pas actés dans la procédure, puisqu'ils sont à un stade éloigné des indices et encore plus des preuves. Dans ces conditions, lorsque des investigations sont éparpillées entre plusieurs services, notamment pour des questions géographiques, ou entre des intervenants différents tels que des experts commis, ce savoir, qui ne s'est pas traduit (ou pas encore traduit) par des résultats et donc des procès-verbaux, ne parvient pas jusqu'aux intervenants ponctuels dans la procédure et ne peut donc pas être mobilisé pour les investigations correspondantes. La conséquence qui en découle est qu'un élément important peut échapper à ces enquêteurs ou cet expert.

775. L'importance du « savoir » en matière d'investigation numérique. – Cette situation prend toute son importance avec la dissémination des investigations numériques, car les recherches par mots clés[1281] sont essentielles pour toutes les analyses conduites sur les données issues de supports numériques. Or, pour que la personne procédant à l'analyse soit en mesure d'utiliser les bons mots clés dans les recherches, l'entier savoir de l'enquête peut s'avérer déterminant et pas seulement les pièces de procédure transmises lors de la saisine d'un enquêteur géographiquement distant ou d'un expert[1282].

776. Dans ce contexte, le fait de confier différentes investigations numériques à des intervenants distincts, sans lien entre eux, autres que les pièces de la procédure, nuit à l'efficacité de l'enquête.

[1279] Un groupe de travail, dirigé par Jean-François ABGRALL avait été créé au sein de la section de recherche de la gendarmerie de Rennes pour l'enquête relative au tueur en série Francis HEAULME. Dans le cadre de la disparition de la jeune Marion WAGON le 14 novembre 1996, une « cellule Marion » a été créée au sein de la section de recherche de la gendarmerie d'Agen. Celle-ci a compté jusqu'à 40 enquêteurs.
[1280] Ces intuitions ou ces soupçons ne sont pas forcément dirigés à l'encontre d'un suspect, mais peuvent concerner tous les éléments matériels de l'enquête tels que le *modus operandi*, les déclarations des victimes, etc.
[1281] V. *supra* n°762.
[1282] A savoir le rapport ou le procès-verbal. V. *supra* n°757.

§2. L'efficacité freinée par les intervenants différents

777. La multiplication des intervenants procédant à des investigations numériques. – L'efficacité des investigations numériques est bridée par le cloisonnement des données qui sont analysées acte par acte. Cumulativement, ce frein est amplifié lorsque ces actes sont confiés à des personnes différentes. En effet, cet éparpillement entre des intervenants différents ne permet pas de capitaliser et, *a fortiori*, d'utiliser, le savoir qui se constitue au sein d'une enquête.

778. Par exemple, il est fréquent qu'un enquêteur spécialisé en criminalité informatique procède à l'analyse d'un téléphone au cours de la garde à vue d'un suspect, tandis qu'un expert analyse les ordinateurs saisis lors d'une perquisition, et que des officiers de police judiciaire procèdent à des recherches dans les fichiers correspondants à des factures téléphoniques obtenues en réponse à une réquisition[1283].

779. L'incompatibilité entre l'enquête numérique et la multiplicité des intervenants. – Le savoir qui s'accumule au fur et à mesure de l'avancée d'un dossier est particulièrement important en matière d'investigation numérique.

Les interventions multiples dont, tout particulièrement, celles des experts, posent un problème spécifique, non seulement en rompant l'utilisation de ce savoir, mais également en freinant l'enchaînement et l'imbrication des différentes mesures procédant à des investigations sur des données *(I)*.

Ainsi une sorte d'enquête numérique doit pouvoir se créer au sein de l'enquête proprement dite *(II)*.

I – Le frein à l'enchaînement des investigations numériques

780. La multiplication des intervenants procédant à des investigations numériques due à différentes situations. – Outre l'exemple précédent[1284], la dissémination des investigations auprès de personnes différentes peut avoir plusieurs origines.

781. En premier lieu, la dissémination la plus évidente découle de l'indisponibilité d'un enquêteur spécialisé[1285] ou des contraintes géographiques imposant d'enquêter dans un

[1283] V. *supra* n°372.
[1284] V. *supra* n°778.
[1285] Par exemple, en matière d'investigation numérique, l'indisponibilité du N'Tech (v *supra* n°323.) d'un département peut conduire à ce que ce soit un N'Tech d'un département limitrophe qui procède à des analyses sur des supports numériques.

lieu éloigné. Dans ces deux cas, les enquêteurs prennent généralement contact avec ceux initialement saisis, voire même, dans les dossiers très sensibles, n'hésitent pas à se déplacer pour travailler ensemble. Le savoir de l'enquête est alors transmis et sa continuité est assurée.

782. L'intervention des experts. – En second lieu, l'origine de l'intervention de personnes différentes découle directement de la commission ou de la réquisition des experts judiciaires[1286]. Ces derniers ont déjà longuement été évoqués puisque leur intervention est souvent obligatoire pour analyser des scellés[1287]. Or, l'intervention d'un expert judiciaire « civil[1288] » au sein de la procédure incarne la rupture dans l'utilisation du savoir de l'enquête[1289] pour procéder aux investigations correspondantes.

783. Le savoir de l'enquête essentiel pour les investigations numériques. – Cette rupture dans l'utilisation du savoir revêt un aspect particulièrement critique lorsqu'il s'agit d'analyser des supports numériques. En effet, les investigations sur les supports numériques ont une particularité qui accentue le frein à l'efficacité de l'enquête, lorsque l'analyse est réalisée par un intervenant qui ne dispose pas de l'intégralité du savoir de l'enquête, comme c'est le cas avec un expert civil. Dès que des données sont à analyser, que celles-ci proviennent d'un smartphone ou dans un ordinateur, la mission donnée par le juge est ouverte[1290], ce qui signifie que l'expert doit procéder à une « mini enquête[1291] » au travers des investigations diligentées sur le support[1292]. Lors de l'analyse, notamment des fichiers cachés, des dossiers renommés pour tenter de les dissimuler, mais surtout en procédant à des recherches par mots clés[1293], l'expert doit révéler ou reconstituer une partie de la « vie numérique » de l'utilisateur de l'ordinateur. Il ne s'agit en rien de minimiser l'importance et la complexité des autres expertises techniques, mais de relever la particularité des analyses de supports numériques qui conduisent la personne qui

[1286] V. *supra* n°300.
[1287] V. *supra* n°325.
[1288] Le mot « civil » est employé pour différentier les experts issus de la société civile des gendarmes ou des policiers qui sont inscrits sur les listes d'experts. V. *supra* n°341.
[1289] V. *supra* n°775.
[1290] Par ex., dans les ordonnances de commission d'expert, les juges d'instruction emploient très souvent la formule : « rechercher tous les éléments en rapport avec les faits ».
[1291] En 2008, Karline BOUISSET, alors juge d'instruction au Tribunal de Grande Instance d'Albi disait que « l'expert en informatique doit avoir l'âme de l'enquêteur ».
[1292] On peut retrouver une certaine similitude avec les expertises comptables complexes ou l'expert, pour mettre à jour des faits répréhensibles, doit se mettre dans cette logique de mini-enquête en se plongeant dans les données comptables et financières d'une structure.
[1293] V. *supra* n°762.

diligente les investigations sur le support donné, à procéder à une sorte d'enquête numérique. Le périmètre initialement défini pour la mission est beaucoup plus ouvert que pour des expertises telles que les analyses chimiques ou génétiques.

784. Le périmètre d'intervention de l'expertise fortement limité. – Cette sorte d'enquête numérique met en évidence que la réquisition ou la commission d'un expert, visant à lui confier l'analyse du contenu d'un support numérique, est inadaptée au besoin de continuité que nécessitent les investigations numériques. En effet, dans les années 1990 jusqu'au milieu des années 2000, les expertises informatiques fonctionnaient, techniquement, de la même manière que les autres expertises. Un disque dur ou un ordinateur était saisi lors d'une perquisition, puis son contenu était analysé par un expert qui remettait, *in fine*, un rapport. Ce système fonctionnait bien puisque l'analyse de ces supports numériques était autonome, dans le sens où les données présentes permettaient à l'expert de mener à bien sa mission en autonomie.

785. Or, la dématérialisation intense que connait notre société[1294] depuis une dizaine d'année avec l'importance des réseaux sociaux et le *cloud*[1295], a considérablement modifié le stockage des informations. Désormais, les données susceptibles d'être présentes sur les disques durs des ordinateurs ou au sein des tablettes et autres smartphones, ne prennent sens qu'en liaison avec des forums, des réseaux sociaux ou des espaces de stockage accessibles au travers d'Internet. L'exemple le plus intuitif concerne la consultation des sites Internet nécessitant une authentification. Bon nombre de ces sites, de type forum, cumulent des fonctions d'espace d'échange et de partage de fichiers. Les réseaux pédophiles utilisent largement ce type de sites, souvent hébergés en Russie ou dans des pays d'Europe de l'est.

786. L'expert qui analyse le disque dur d'un individu surfant régulièrement sur un tel forum, peut, certes, retrouver les liens vers les pages consultés, et peut, sous certaines conditions[1296], retrouver quelques images, mais, sauf situation rarissime[1297], il ne va pas pouvoir se rendre au sein du forum. Plus généralement, l'expert peut utiliser tous les moyens techniques dont il dispose pour casser ou contourner des mots de passe lui

[1294] V. *supra* n°16.
[1295] V. *supra* n°221.
[1296] Si les caches du navigateur sont régulièrement effacés, les chances de retrouver des images complètes et représentatives s'amenuisent considérablement.
[1297] Que les identifiants de connexion soient enregistrés dans le navigateur de sorte que, lorsque le technicien qui procède à l'analyse, clique sur le lien il se trouve automatiquement identifié sur le forum.

permettant d'accéder aux informations enregistrées dans le support numérique dont l'analyse lui est confiée mais, en aucun cas, le cadre légal de l'expertise ne l'autorise à utiliser les mêmes outils pour pénétrer sur des sites ou des espaces de stockage en ligne fermés. S'il faisait cela, il commettrait une infraction[1298].

787. L'inefficacité de l'analyse isolée d'un support. – Cette sorte d'enquête numérique impose donc que l'analyse d'un scellé contenant des données puisse être prolongée par d'autres investigations numériques, et ceci avec un besoin fort de continuité temporelle.

II – La nécessité d'une enquête numérique au sein de l'enquête

788. Un besoin de continuité entre les différentes investigations numériques. – Pour être efficace, l'enquête numérique repose sur l'exploitation du savoir qui se crée au sein de l'enquête. Certes, ce dernier est utile à l'enquête dans son ensemble. Néanmoins, par rapport à d'autres actes technologiques[1299], les investigations numériques ont une particularité qui consiste en un enchaînement et une complémentarité forte des différentes investigations numériques les unes par rapport aux autres. Ainsi, lorsque l'analyse d'un scellé est confiée à un expert, celui-ci se trouve rapidement bloqué car, les données présentes sur le support analysé imposent le plus souvent de devoir accéder, au travers d'Internet, à des sites ou des espaces de stockages dans le *cloud*.

789. Le prolongement de l'analyse d'un support numérique. – L'analyse d'un support numérique peut nécessiter, par exemple, de procéder à une enquête sous pseudonyme[1300], ou une perquisition en ligne[1301], qui sont des actes que l'expert ne peut pas accomplir. Dans le cadre de l'enquête sous pseudonyme, seuls des enquêteurs dument

[1298] C. pén. art. 226-4-1 et 434-23 récriminant l'usurpation d'identité.
VERNY Edouard, *Usurpation d'identité,* JurisClasseur Communication, Fasc. 58.
MONTEIL Marine, *L'usurpation d'identité à l'épreuve du numérique*, Recueil Dalloz 2020 p.101 : « Lorsque l'usurpation d'identité est pratiquée sur les réseaux de communication au public en ligne, elle est souvent qualifiée de « délit d'usurpation d'identité numérique ». Or le droit pénal ne connaît qu'un seul délit : l'usurpation d'identité. Le fait que l'infraction soit commise dans le monde réel ou dans l'univers dématérialisé ne modifie ni l'élément matériel ni l'élément moral requis. »
[1299] C. pr. pén. art. 230-46 - V. *infra* n°792.
[1300] C. pr. pén. art. 57-1 - V. *supra* n°468.
[1301] V. *supra* n°250.

habilités[1302] peuvent exécuter cette mesure. Dans le cas de la perquisition en ligne, sa mise en œuvre est évidemment réservée aux autorités judiciaires. Tout au plus, l'expert pourrait accompagner les enquêteurs si une réquisition ou une ordonnance de commission d'expert lui confiait une mission en ce sens.

790. La perquisition en ligne devient nécessaire dans le cas, notamment, d'un espace de stockage en ligne[1303]. Des personnes peuvent intentionnellement stocker des fichiers dans l'un des multiples espaces de stockage qui sont gratuitement offerts par des « géants » du *web*[1304] et n'enregistrer aucun fichier localement sur les outils numériques qu'ils utilisent. Lors des perquisitions, les enquêteurs ont la possibilité d'accéder à de telles données[1305], ce qui n'est pas le cas de l'expert. Il ne peut pas, légalement, procéder à des recherches sur de tels espaces de stockage, même s'il constate au travers des données présentes sur le disque dur soumis à l'expertise que l'utilisateur de l'ordinateur s'y connectait.

791. La nécessité d'utiliser un ensemble d'investigations numériques pour enquêter au sein de l'espace numérique d'un individu. – Ces différentes illustrations confirment la liaison, précédemment évoquée, entre les objets numériques physiquement détenus par un individu et les données stockées à de multiples endroits sur Internet, dont l'utilisateur de ces objets peut être le propriétaire[1306] ou qui illustrent qu'il est un participant actif d'un espace collaboratif. Le disque dur ou la mémoire du smartphone ne contiennent qu'une petite partie des données constituant l'espace numérique généré par une personne. Or, pour que l'enquête numérique soit efficace, elle doit pouvoir faire appel à un ensemble d'investigations numériques permettant d'enquêter dans l'intégralité de cet espace numérique. Dès lors, l'expertise traditionnelle qui consiste à confier à un expert l'analyse d'un ordinateur risque, le plus souvent, de freiner considérablement l'efficacité de la procédure. En effet, pour avoir la capacité d'enquêter dans l'intégralité de l'espace

[1302] C. pr. pén. art. 230-46 : « […] les officiers ou agents de police judiciaire agissant au cours de l'enquête ou sur commission rogatoire peuvent, s'ils sont affectés dans un service spécialisé et spécialement habilités à cette fin […]. »
[1303] C'est-à-dire un espace de stockage mis à disposition par un prestataire extérieur et auquel il est possible d'accéder de manière nomade *via* Internet.
[1304] Google drive, Onedrive de Microsoft, etc.
[1305] V. *supra* n°250.
[1306] Stockage de fichiers.

numérique généré par un individu, c'est un ensemble d'investigations numériques qui doivent être actionnées avec une forte continuité temporelle, voire même en parallèle[1307].

792. A titre de comparaison, les résultats d'une analyse chimique ou biologique peuvent, bien évidemment, orienter l'enquête vers de nouvelles pistes, mais, à la différence de l'analyse d'un support numérique, il n'y a pas d'interaction aussi forte avec d'autres investigations[1308]. Dans l'exemple précédent, le numéro de téléphone retrouvé lors de l'analyse d'un disque dur va déclencher une réquisition pour connaître le titulaire de la ligne[1309]. Mais, le nom ainsi obtenu enrichit les possibilités d'analyse du disque dur puisque l'enquêteur peut procéder à des recherches par mots clés sur celui-ci. Il y a donc une imbrication forte entre les analyses de supports numériques et les autres investigations numériques. Au-delà d'une imbrication, elles sont même souvent entrelacées.

793. Dans les cas extrêmes, comme en matière de terrorisme, l'analyse d'un ordinateur doit pouvoir se prolonger par des investigations au sein de forums puisque plusieurs infractions s'intéressent au terrorisme et aux réseaux de communication en ligne[1310]. Les éléments recueillis au travers de ce type de publication sont utiles pour caractériser le degré d'activisme et de radicalisme d'un individu. Or, les investigations numériques comportent des spécificités telles que la volatilité des données[1311] qui impose que tous les actes permettant de collecter l'ensemble des preuves numériques soient réalisés de manière fluide et coordonnée, afin de ne pas prendre le risque que, par exemple, les publications sur un forum soient effacées, avant qu'elles aient pu être constatées par un officier de police judiciaire.

794. Une incompatibilité prise en compte par les pouvoirs publics. – Il se dégage une contradiction importante au sein de la procédure pénale en matière d'investigations numériques entre des règles qui, historiquement, accordent un rôle essentiel aux experts judiciaires[1312] pour analyser des supports numériques, et des dispositions qui sont

[1307] Par ex., la réquisition d'un opérateur (v. *supra* n°372.) pour obtenir les coordonnées administratives déclarées par l'utilisateur d'une adresse électronique, peut être réalisée en même temps que la mise sur écoute d'une ligne téléphonique (v. *supra* n°528.) dont le numéro a été retrouvé dans le carnet d'adresse présent dans un ordinateur.
[1308] SAVART Michel (Directeur du laboratoire de police scientifique de Lyon), *L'expertise scientifique en matière pénale,* Dalloz AJ pénal 2006 p. 72.
[1309] Sur l'obtention d'informations numériques auprès de tiers, V. *supra* n°372.
[1310] C. pén. art. 421-2-5, art. 421-2-5-1 ou encore l'art. 421-2-6.
[1311] V. *supra* n°223.
[1312] V. *supra* n°782.

réservées aux enquêteurs. Cette contradiction est accentuée par la volatilité des données qui impose que les investigations numériques soient diligentées de manière synchronisées et avec rapidité.

795. En conséquence, seuls les enquêteurs de la Police ou de la Gendarmerie peuvent mener avec efficacité cette sorte d'enquête numérique, obligeant ainsi à repenser les interventions des experts en informatique[1313]. Or, outre les longs délais traditionnellement en vigueur pour une expertise informatique de ce type[1314], le fait que les enquêteurs fassent tout pour contourner la saisine d'un expert civil[1315] illustre l'inadéquation de cet acte de procédure avec les contraintes des investigations numériques.

796. La démonstration que cette façon de procéder ne répond pas aux besoins de cette sorte d'enquête numérique est parfaitement concrétisé par l'introduction de l'article 60-3 dans le Code de procédure pénale par la loi du 3 juin 2016[1316]. Cet article prévoit la possibilité de faire appel à un expert pour cloner des supports numériques saisis, afin que les enquêteurs puissent procéder à des investigations sur l'image des données ainsi réalisée[1317]. Les enquêteurs utilisent énormément cette façon de procéder[1318]. L'objectif est de disposer d'un maximum de réactivité et donc de pouvoir mettre en œuvre l'enchaînement et l'imbrication des différentes investigations numériques, tel que cela vient d'être évoqué.

797. Conclusion de la section 2 : la dissémination des données auprès d'intervenants différents. – Au cours d'une procédure, un savoir se capitalise au fur et à mesure que progresse l'enquête. Celui-ci est déterminant pour les investigations numériques puisqu'il conditionne directement l'efficacité des recherches par mots clés.
Or, lorsque des investigations numériques sont confiées à différents intervenants au sein d'une même procédure, le savoir de l'enquête n'est pas mobilisé ce qui peut nuire à la qualité des recherches.

798. Conclusion du chapitre 1 : l'efficacité des investigations numériques entravée par le cloisonnement des données. – L'éparpillement des investigations numériques

[1313] V. *infra* n°930.
[1314] Entre deux et quatre mois.
[1315] Des enquêteurs de l'IRCGN ou des laboratoires de la Police sont inscrits en leur nom propre sur les listes d'experts. V. *supra* n°341.
[1316] Loi n°2016-731 du 3 juin 2016. *Op. cit. p.23*
[1317] V. *supra* n°348.
[1318] V. *supra* n°350.

auprès d'intervenants différents contribue au cloisonnement des données obtenues avec des actes intrusifs. En effet, les données qui sont exploitées par des personnes différentes ne sont pas analysées ensemble. Cet éparpillement accentue le cloisonnement des données qui découle de la séparation des actes. Cette dernière empêche la possibilité d'analyser, en les regroupant, les données obtenues avec les différentes investigations numériques. Cette impossibilité est un frein à l'efficacité des investigations numériques, puisque l'exploitation conjointe de toutes les données obtenues au travers des actes intrusifs améliorerait leur analyse.

Chapitre 2. L'efficacité des investigations numériques améliorée par le regroupement des données

799. La nécessité de regrouper les données obtenues par les actes intrusifs. – Les investigations numériques sont des actes de procédure qui conduisent à l'obtention de données[1319]. Parmi ces investigations, les actes intrusifs forment la première catégorie[1320]. L'efficacité des mesures composant cette dernière est bridée par le cloisonnement des données obtenues. La possibilité de procéder à une analyse des données regroupées de toutes les investigations numériques réalisées au sein d'une enquête constitue un enjeu majeur[1321] pour améliorer l'exploitation des informations obtenues sous forme numérique.

800. La proposition de modifications pour regrouper les données obtenues. – La présente étude propose des modifications légales et règlementaires qui permettraient de répondre à cet enjeu. Elles consisteraient à introduire un acte nommé « le traitement d'exploitation judiciaire ».
La création de cet acte *(Section 1)* et sa mise en œuvre *(Section 2)* sont étudiées distinctement.

[1319] V. *supra* n°194.
[1320] V. *supra* n°283.
[1321] V. *supra* n°82.

Section 1. Le regroupement des données par la création du « traitement d'exploitation judiciaire »

801. La nécessité d'une consolidation régulière et continue des données. – Le « traitement d'exploitation judiciaire (ci-après TEJ) » est un acte qui pourrait être créé avec comme objectif de pouvoir regrouper les données au fur et à mesure qu'elles sont collectées par les enquêteurs, afin qu'elles puissent être analysées ensemble. Par exemple, les données issues d'un disque dur d'ordinateur seraient associées à celles présentes dans un téléphone, ainsi qu'avec les fichiers audio provenant d'une écoute téléphonique. L'enquêteur exploiterait alors cet ensemble de données. Or, cette façon de procéder se heurte au principe de séparation des actes les uns par rapport aux autres[1322]. L'étude de la création du traitement d'exploitation judiciaire nécessite donc d'envisager des modifications qui devraient être apportées à la procédure pour pouvoir parvenir à l'analyse regroupée des données. Néanmoins, l'étude des modifications n'est pas suffisante. En effet, lorsque cette mesure entrerait dans ses effets, un risque juridique nouveau apparaîtrait. Celui-ci découlerait d'éventuelles nullités frappant des actes ayant fourni des données exploitées conjointement à celles d'autres mesures.

802. En conséquence, il est nécessaire de distinguer l'étude du cadre légal permettant de créer le traitement d'exploitation judiciaire *(§1)* et les risques de l'effet de la nullité de l'une des investigations numériques ayant alimenté en données le TEJ mis en œuvre pour cette enquête *(§2)*.

§1. Le cadre légal du traitement d'exploitation judiciaire

803. Les logiciels de rapprochement judiciaire comme base d'évolution. – Depuis 2011[1323], il est possible pour des enquêteurs habilités de regrouper les données et les informations provenant de différentes sources au sein d'une même procédure, en utilisant les « logiciels de rapprochement judiciaire[1324] ». Ainsi, il semble que la possibilité d'analyser, ensemble, des données issues de plusieurs actes différents soit déjà prévue. Toutefois, les dispositions actuelles définissant cet acte, ne répondent pas pleinement à l'objectif qui vient d'être décrit, car certaines limitations ressortent de la formulation des

[1322] V. *supra* n°755.
[1323] Loi n°2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure.
[1324] C. pr. pén. art. 230-20 et s. – Pour une description des logiciels de rapprochement judiciaires : v. *supra* n°720. et annexe 1, fiche A1/20.

textes. De plus, il existe une confusion importante au sein de la procédure pénale, dans la distinction erronée qui est faite entre les traitements de données personnelles et l'analyse des données contenues dans un scellé, par les enquêteurs ou les experts[1325].

804. Avant de proposer les modifications des logiciels de rapprochement judiciaire permettant d'analyser toutes les données issues d'actes différents *(II)*, il est, préalablement, nécessaire de comprendre cette confusion *(I)*, car la création du TEJ souffre directement de cette incohérence.

I – L'incohérence entre les traitements de données personnelles et l'analyse des données

805. Une distinction erronée due à des raisonnements différents. – Au sein de la procédure pénale, deux raisonnements différents cohabitent pour traiter les données issues des investigations numériques. En premier lieu, l'analyse de supports numériques contenant des données ayant été mis sous scellés[1326], traite les données comme n'importe quel autre élément contenu dans un scellé. Le raisonnement pour analyser les informations numériques contenues dans ce scellé s'inscrit dans la conception historique de l'exploitation de celui-ci.

806. En second lieu, les actes créés plus récemment pour procéder à d'autres investigations numériques, telles que la captation des données informatiques[1327], l'interception de correspondances émises par la voie de communication électronique[1328], ou encore les logiciels de rapprochement judiciaire[1329], adoptent le raisonnement de la mise en œuvre d'un traitement de données à caractère personnel[1330].

807. Or, une telle distinction dans la perception qui est faite, par la procédure, des données exploitées, est erronée et totalement injustifiée. Lorsque, par exemple, un ensemble de supports numériques saisis lors d'une perquisition à analyser sont confiés à un expert, ces supports contiennent évidemment des données à caractère personnel, notamment au travers des messageries et des fichiers créés par l'utilisateur de l'appareil.

[1325] V. *supra* n°293.
[1326] *Ibid.*
[1327] C. pr. pén. art. 706-102-1 et s. V. *supra* n°692.
[1328] V. *supra* n°687. La PNIJ est le traitement de données permettant la mise en œuvre opérationnelle des écoutes téléphoniques (C. pr. pén. art. 230-45).
[1329] C. pr. pén. art. 230-20 et s. V. *supra* n°720.
[1330] Sur la notion de traitement de données à caractère personnel, v. *supra* n°609.

L'expert utilise alors des outils d'analyse *forensique*[1331], sur l'ensemble des données contenues dans les supports qui lui sont confiés. Au travers de ces outils, notamment avec la fonction d'indexation[1332], un traitement de données personnelles au sens du RGPD[1333] est ainsi créé[1334]. C'est tout particulièrement le cas au travers des recherches par mots clés, qui constituent un traitement des données personnelles saisies.

808. L'exploitation des scellés contenant des données inextricablement associée à la mise en œuvre d'un traitement de données personnelles. – Les analyses des scellés contenant des supports numériques manipulent donc des données à caractère personnel tout autant que les investigations numériques créées récemment. Or, ces dernières reposent sur la création d'un traitement à caractère personnel[1335], alors que les analyses des scellés font abstraction de la notion de données personnelles. Parmi ces investigations numériques comportant la mise en œuvre explicite d'un traitement de données, les « logiciels de rapprochement judiciaire[1336] » permettent de comprendre l'incohérence dans la différence de raisonnement sur cette appréhension des données au sein de la procédure pénale.

809. Des régimes actuellement différents. – En effet, la conséquence de cette différence de raisonnement se traduit par des régimes hétérogènes relatifs aux données issues de deux investigations numériques, pourtant, très proches dans leurs effets : l'exploitation des informations numériques. Ces différents régimes ne doivent pas être confondus avec la pluralité des régimes étudiées précédemment[1337], qui concernait la mise en œuvre et les effets des investigations numériques. La présente partie s'intéresse aux données obtenues grâce à ces dernières[1338]. Ainsi, les analyses de scellés contenant

[1331] V. *supra* n°761.
[1332] L'indexation consiste à créer une base de données locale avec les informations contenues sur le support analysé : v. *supra* n°762.
Sur le lien entre l'indexation des informations numériques et la performance des recherches, v. LUSSAN Pierre-Louis, *Respect de la protection de la vie privée : bien plus qu'une simple case à cocher pour les entreprises,* Silicon, 12 dec. 2019.
[1333] *Op. cit.* p.13 - 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).
[1334] *Ibid.* RGPD, art. 4 pour la définition des « données à caractère personnel » et de « traitement ».
[1335] V. *supra* n°806.
[1336] V. *supra* n°35
[1337] V. *supra* n°233.
[1338] V. *supra* n°733.

informations numériques et la mise en œuvre des logiciels de rapprochement judiciaire ont en commun d'autoriser l'analyse des données au sein d'une procédure, mais traitent ces dernières différemment.

810. L'hétérogénéité dans l'encadrement de la mise en œuvre. – En procédure, l'expertise est la voie usuelle pour procéder à l'analyse de données contenues dans un scellé[1339]. Les dispositions encadrant cette mesure ne se préoccupent absolument pas des outils qu'utilise l'expert pour exploiter les données, lui laissant ainsi une grande marge de manœuvre. *A contrario*, les analyses réalisées sur les données dans le cadre du rapprochement judiciaire ne peuvent être accomplies qu'avec des logiciels dûment autorisés[1340], et l'utilisation de ces outils doit faire l'objet d'une autorisation d'un magistrat pour chaque enquête[1341]. Cette autorisation du juge pour la mise en œuvre d'un traitement de données au travers de l'utilisation des logiciels de rapprochement judiciaire est un régime différent pour traiter les données, que celui qui découle de la saisine d'un expert. Ce dernier peut analyser des données après avoir été commis ou réquisitionné[1342], sans se préoccuper qu'il mette en œuvre un traitement de données pour cela.

811. L'hétérogénéité dans l'exploitation intrinsèque des données. – Pour les logiciels de rapprochement judiciaire, c'est le régime des traitements de données personnelles qui s'applique. C'est donc l'utilisation[1343], la conservation et l'effacement des « données à caractère personnel éventuellement révélées[1344] » auxquelles la loi et le règlement s'intéressent. En revanche, une grande liberté, quasi-totale, est laissée aux enquêteurs dans l'exploitation des données qui est faite au travers de ces logiciels. La seule limitation est que les recherches diligentées sur les données soient relatives aux modes opératoires[1345]. L'agent ou le militaire habilité à l'utilisation des logiciels de

[1339] V. *supra* n°299.
[1340] C. pr. pén. art. 230-27 : « Les logiciels faisant l'objet du présent chapitre ne peuvent être autorisés que par décret en Conseil d'Etat pris après avis de la Commission nationale de l'informatique et des libertés. » Au sujet de la déclaration des logiciels : v. *supra* n°723.
[1341] C. pr. pén. art. R40-40.
[1342] V. *supra* n°300.
[1343] Voire leur non-utilisation puisque l'art. 230-26 dispose que « les logiciels […] ne peuvent en aucun cas être utilisés pour les besoins d'enquêtes administratives […] ». Au demeurant, il ressort de cet article une grande contradiction puisqu'une consultation à des fins administratives du Traitement d'Antécédents Judiciaires est prévue (v. *supra* n°648.). Or, il peut y avoir, dans ce traitement, des éléments factuels qui découlent directement du résultat d'investigations accomplies avec les logiciels de rapprochement judiciaire.
[1344] C. pr. pén. art. 230-22.
[1345] V. *infra* n°830.

rapprochement judiciaire[1346] n'est donc pas limité dans ses recherches et, par voie de conséquence, il peut verser à la procédure au travers d'un procès-verbal tout ce qu'il a ainsi découvert. Inversement, en matière d'analyse de données contenues dans un scellé, la mission confiée à l'expert est fortement encadrée, que ce soit par le biais de l'expertise ou de la réquisition. Au stade de l'information judiciaire, cette mission doit même être communiquée aux parties qui peuvent demander des modifications[1347]. L'expert ne peut pas, ainsi, exploiter librement les données contenues dans les supports qu'il analyse. Il doit se limiter à rechercher les éléments définis par la mission qui lui est confiée[1348]. Toutefois, cette règle est souvent considérablement atténuée par le juge, puisque l'usage veut que le dernier alinéa de la mission d'expertise se termine par : « faire toute observation utile à la manifestation de la vérité ». Une grande marge de manœuvre s'ouvre alors pour l'expert.

812. L'hétérogénéité dans la mise en cause de nouvelles personnes. – L'exploitation des données, aussi bien dans le cadre de l'analyse d'un support numérique contenu dans un scellé, qu'au travers des logiciels de rapprochement judiciaire, peut aboutir à mettre à cause une personne jusqu'alors non soupçonnée. Ce cas est explicitement prévu par le deuxième alinéa de l'article 230-21 du Code de procédure pénale relatif aux logiciels de rapprochement judiciaire[1349]. Ces dispositions encadrent avec précision la mise en cause d'un nouvel individu faisant suite aux résultats de l'exploitation de données. Dans le cas de l'analyse d'un scellé, rien de tel n'est prévu. Pourtant, un échange de SMS retrouvé dans un téléphone, ou un courriel présent dans les caches du navigateur d'un ordinateur, peut révéler l'implication d'un tiers, jusque-là ignoré. Le nom mis en évidence peut alors être exploité sans aucun encadrement textuel, ce qui est peu protecteur pour le respect des libertés individuelles.

813. Une nécessaire homogénéisation des régimes. – L'ensemble de ces différences dans l'exploitation des données obtenus au sein d'investigations numériques, pourtant

[1346] C. pr. pén. art. 230-25 : « Peuvent seuls utiliser les logiciels faisant l'objet du présent chapitre […] les agents des services mentionnés à l'article 230-20, individuellement désignés et spécialement habilités, pour les seuls besoins des enquêtes dont ils sont saisis [...]. »

[1347] C. pr. pén. art. 161-1.

[1348] Ex. « Rechercher tous les éléments révélant la consultation de vidéos pornographiques mettant en scène des mineurs. »

[1349] « Lorsque sont exploitées des données pouvant faire indirectement apparaître l'identité des personnes, celle-ci ne peut apparaître qu'une fois les opérations de rapprochement effectuées, et uniquement pour celles de ces données qui sont effectivement entrées en concordance entre elles ou avec d'autres informations exploitées par le logiciel. »

très proches dans les effets, est fortement préjudiciable. En effet, le point en commun des investigations sur des données personnelles est qu'elles sont particulièrement intrusives dans la vie privée d'un ou plusieurs individus. Il est donc regrettable que certaines données soient analysées sous le régime des traitements à caractère personnel, tandis que les données contenues dans des scellés le soient dans un cadre nettement moins protecteur.

814. Ainsi, les propositions de création du traitement d'exploitation judiciaire ont vocation à homogénéiser les deux régimes pour les données obtenues en enquête. Cette homogénéisation contribuerait à l'équilibre entre l'amélioration de l'efficacité de l'enquête et le respect des libertés individuelles.

II – La cohérence rétablie par le traitement d'exploitation judiciaire

815. Des « logiciels de rapprochement judiciaire » au « traitement d'exploitation judiciaire ». – La possibilité d'analyser, ensemble, des données issues de plusieurs actes différents est prévue grâce aux logiciels de rapprochement judiciaire[1350]. Toutefois, cet acte ne permet pas, en l'état, d'exploiter toutes les données issues d'investigations numériques préalablement exécutées, en raison de certaines limitations. Il est donc nécessaire d'étudier la modification des dispositions actuelles encadrant les logiciels de rapprochement judiciaire, pour transformer ces derniers en un « traitement d'exploitation judiciaire » (ci-après « TEJ ») des données. Cette transformation doit être complétée par une adaptation de l'exploitation des scellés afin que les données qu'ils contiennent puissent alimenter le TEJ. Comme précédemment expliqué[1351], la création du TEJ et les modifications des dispositions relatives à l'exploitation des scellés qui en découlent, doivent être accompagnées d'une homogénéisation des différents régimes qui cohabitent actuellement pour l'exploitation des données personnelles obtenues au sein d'une enquête pénale.

816. Les dispositions permettant d'atteindre l'ensemble de ces objectifs doivent être présentées en deux temps. En premier lieu, l'adaptation des logiciels de rapprochement judiciaire pour créer le TEJ représente une première série de dispositions *(A)*. En second lieu, le cadre de l'exploitation des scellés contenant des données doit être modifié *(B)*.

[1350] V. *supra* n°803.
[1351] V. *supra* n°813.

A. L'adaptation des logiciels de rapprochement judiciaire

817. Le détournement de la finalité initiale des logiciels de rapprochement judiciaire. – Initialement, lors de leur création par la loi de 2011[1352], les logiciels de rapprochement judiciaire avaient pour vocation de permettre le regroupement d'informations issues de procédures différentes. Or, le Conseil constitutionnel a restreint cette possibilité *(1)*. Cette importante limitation, qui a laissé cet acte dans une sorte d'état instable, offre désormais une opportunité pour étendre cette mesure au-delà de sa finalité originelle afin de créer le traitement d'exploitation judiciaire des données *(2)*.

1. La restriction de la finalité des logiciels de rapprochement judiciaire

818. L'objectif initial calqué sur les fichiers d'analyse sérielle. – Les fichiers d'analyse sérielle et les logiciels de rapprochement judiciaires ont été créés par la même loi de 2011 et sont très proches[1353]. L'objectif initial des logiciels de rapprochement judiciaire était de créer une base de données transversale aux différentes procédures dont sont issues les informations. En effet, les dispositions encadrant les traitements résultant de la mise en œuvre des logiciels de rapprochement judiciaire[1354] sont vagues et pourraient laisser penser qu'ils permettent de faire, pour les petites infractions, ce que les fichiers d'analyse sérielle mettent en place pour les crimes en série, à savoir une base de données nationale collectant des informations issues d'une multitude de procédures. La rédaction « lacunaire [du] cadre juridique [des] logiciels de rapprochement judiciaire[1355] » allait dans le sens des « espoirs portés par les services[1356] » pour créer, au travers de cet outil, un traitement comparable à la base nationale et transversale qui met en œuvre les fichiers d'analyse sérielle, mais utilisable pour « les faits de petite et moyenne délinquance[1357] ». En effet, les fichiers d'analyse sérielle sont réservés à des

[1352] Loi du 14 mars 2011, *op. cit.* p.35
[1353] V. *supra* n°720.
Annexe 1, fiche A1/21. C. pr. pén art. 230-12 et s. – R40-35 et s.
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 ».
Annexe 1, fiche A1/20. C. pr. pén. art. 230-20 et s. – R40-39 et s.
Décret n°2012-687 du 7 mai 2012 relatif à la mise en œuvre de logiciels de rapprochement judiciaire à des fins d'analyse criminelle.
[1354] *Ibid.*
[1355] *Op. cit.* p.35. BATHO Delphine et BENISTI Jacques-Alain, *rapport d'information sur la mise en œuvre des conclusions de la mission d'information sur les fichiers de police,* enregistré le 21 décembre 2011 : p. 33.
[1356] *Ibid.*
[1357] *Ibid.*

infractions punies d'au moins cinq ans d'emprisonnement[1358], tandis que les logiciels de rapprochement judiciaire peuvent être utilisés au sein de toutes les enquêtes ou commissions rogatoires[1359].

819. Un objectif initial anéanti. – Dans sa décision du 10 mars 2011, le Conseil constitutionnel a posé une importante restriction au rapprochement judiciaire en imposant que les traitements de données correspondants ne soient mis en œuvre que « dans le cadre d'une enquête ou d'une procédure déterminée portant sur une série de faits et pour les seuls besoins de ces investigations[1360] ». Concrètement, les fichiers d'analyse sérielle reposent sur une base de données nationale regroupant des informations issues de différentes procédures présentant, ou susceptibles de présenter, un caractère répété à travers le territoire, tandis que, suite à la décision du Conseil, les logiciels de rapprochement judiciaire permettent uniquement de rassembler les informations d'une seule et même procédure.

820. Les limitations formulées par le Conseil ont été retranscrites par les autorités publiques dans un décret du 7 mai 2012[1361]. Ce décret explicite clairement que seules les informations « réunies au cours d'une même enquête » peuvent être exploitées au sein des logiciels de rapprochement judiciaire.

821. L'utilisation du frein aux logiciels de rapprochement judiciaire. – Le Conseil constitutionnel a considérablement bridé les objectifs initiaux des logiciels de rapprochement judiciaire. Leur utilisation doit être limitée aux données issues d'une seule et même procédure. Cette limitation fait de cet outil d'enquête une base particulièrement bien adaptée à la création du traitement d'exploitation judicaire.

[1358] C. pr. pén. art. 230-12.
[1359] C. pr. pén. art. 230-20.
[1360] Conseil constitutionnel, décision n°2011-625 DC du 10 mars 2011 : considérant n°71.
V. RIBEYRE Cédric, *LOPPSI II : de nouvelles règles au service de la répression,* LexisNexis, Droit pénal n° 7-8, Juillet 2011, étude 10.
[1361] Décret n°2012-687 du 7 mai 2012 relatif à la mise en œuvre de logiciels de rapprochement judiciaire à des fins d'analyse criminelle, article 1 : « […] l'exploitation et le rapprochement d'informations sur les modes opératoires réunis au cours d'une même enquête par les unités de gendarmerie et les services de police chargés d'une mission de police judiciaire […]. »

2. L'extension de la finalité des logiciels de rapprochement judiciaire

822. Une limitation qui offre les prémices d'une réponse au regroupement des données. – La restriction formulée par le Conseil constitutionnel crée opportunément une solution pour procéder à une analyse des données consolidées de tous les actes accomplis au sein d'une procédure. En effet, les logiciels de rapprochement judiciaire prévoient que des « pièces et documents[1362] » provenant de toute la procédure en cours puissent être « exploitées et rapprochées[1363] ». « Pièces et documents » couvrent sans ambiguïté des données qui sont obtenues lors de l'exécution d'actes précédents, et les notions d'exploitation et de rapprochement autorisent une analyse des informations ainsi consolidées.

823. Des projets de textes pour énoncer les modifications nécessaires. – Toutefois, les dispositions[1364] telles qu'elles sont issues de la loi de 2011 nécessitent d'être modifiées, car certains verrous ne permettent actuellement pas d'analyser tout type d'information numérique. Pour concrétiser ces modifications, les dispositions à adapter sont à la fois du ressort de la loi et du règlement[1365]. Deux projets de textes sont donc nécessaires.

824. Une proposition de loi générale. – Les propositions de modification des dispositions législatives font l'objet d'un chapitre premier intitulé « dispositions relatives aux traitements d'exploitation judiciaire » d'une proposition de loi placée en annexe 2 des présentes. Ce projet de texte, nommé « proposition de loi visant à améliorer l'efficacité et à renforcer les garanties des traitements de données en procédure pénale » dépasse l'adaptation des logiciels de rapprochement judiciaire car il comporte un second chapitre relatif à d'autres propositions de modifications de la procédure pénale, également destiné à améliorer l'exploitation des données manipulées lors des investigations numériques[1366]. A ce stade, cette proposition de loi est rédigée comme un texte autonome, mais celle-ci pourrait être insérée dans une loi plus globale relative à la criminalité et

[1362] C. pr. pén. art. 230-21.
[1363] C. pr. pén. art. 230-20.
[1364] C. pr. pén. art. 230-20 et s. – R40-39 et s. – V. annexe 1, fiche A1/20.
[1365] *Ibid.*
[1366] V. *infra* n°1079.

comportant un titre, selon une expression récemment utilisée, visant à « améliorer l'efficacité et à renforcer les garanties de la procédure pénale[1367] ».

825. Un projet de décret dédié au traitement d'exploitation judiciaire. – Conjointement, un projet de décret, objet de l'annexe 3, est nécessaire pour proposer des modifications des différentes dispositions issues du règlement. Outre la partie règlementaire du Code de procédure pénale, le décret du 7 mai 2012 relatif à la mise en œuvre des logiciels de rapprochement judiciaire[1368] devrait être annulé et remplacé. En effet, le décret de 2012 étant entièrement consacré aux logiciels de rapprochement judiciaire, l'adaptation la plus rigoureuse consiste à en proposer son abrogation[1369] pour le remplacer par un décret qui en reprend les dispositions, mais réorientées vers la création du traitement d'exploitation judiciaire. Ce texte est donc naturellement intitulé « projet de décret relatif à la mise en œuvre des traitements à des fins d'exploitation et de rapprochement judiciaires ». Une solution qui consisterait à changer uniquement le titre du décret de 2012 et adapter son contenu, engendrerait une instabilité puisque l'objet du texte modifié et la notice issue du texte initial se contrediraient. Un tel projet de décret doit être préalablement soumis à l'avis de la CNIL[1370].

826. L'importance de la dénomination. – Une première modification consisterait à changer l'appellation « des logiciels de rapprochement judiciaire » qui est utilisée comme titre de deux chapitres du Code de procédure pénale[1371]. Comme précédemment évoqué à propos des fichiers de police judiciaire, il est regrettable que le nom d'un traitement de données ne soit pas représentatif des informations collectées[1372]. En conséquence, il est nécessaire de changer le nom. Tout d'abord, ce dernier est trop restrictif en ne visant que le rapprochement judiciaire, puisqu'il est désormais envisagé de permettre, au travers de ces dispositions, des analyses de données identiques à celles réalisées lors de l'exploitation des supports numériques précédemment mis sous scellés[1373]. Ensuite, ce

[1367] V. par ex. 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.
[1368] Décret n°2012-687 du 7 mai 2012 relatif à la mise en œuvre de logiciels de rapprochement judiciaire à des fins d'analyse criminelle.
[1369] Annexe 3, projet de décret relatif à la mise en œuvre des traitements à des fins d'exploitation et de rapprochement judiciaires, article 1.
[1370] Loi informatique et libertés modifiée par l'ordonnance du 12 décembre 2018 (*op. cit.*), art.31.
[1371] L'un dans la partie législative et le chapitre correspondant dans la partie règlementaire.
[1372] V. notamment *supra* n°655.
[1373] V. *supra* n°807.

titre contient, dès son origine avec la loi de 2011, une incohérence avec tous les autres traitements de données judiciaires. En effet, la quasi-totalité sont désignés[1374] par « fichier », « traitement », voire « répertoire », mais en aucun cas par l'outil informatique qui concrétise la mise en œuvre les traitements de données correspondants.

827. Un nom initial qui va à l'encontre de la loi informatique et libertés. – Le fait de désigner ces traitements par les logiciels va à l'encontre de l'esprit de la loi informatique et libertés[1375] dont l'objectif principal est de protéger la personne concernée par les données collectées, à savoir, notamment, l'utilisation que le responsable du traitement en fait, et à qui il les communique potentiellement. Ainsi, par exemple, qu'un fichier client soit construit dans une base de données Oracle et que dans l'avenir, les données soient basculées dans une base MySQL ne change rien si la nature des données et leur exploitation restent identiques.

828. La proposition de loi de l'annexe 2 propose donc de rectifier cette incohérence en introduisant le mot « traitement ». Celui-ci est conforme au nouvel objectif donné à cet acte d'investigation puisque toutes les analyses actuellement accomplies sous le régime des expertises et des réquisitions d'expert manipulent incontestablement des données à caractère personnel[1376]. De plus, le mot « traitement » a une signification juridique large. Les juridictions ont, notamment, une interprétation très extensive de celui-ci[1377] lorsqu'elles appliquent les infractions relatives aux systèmes de traitement automatisé de données[1378]. Par ailleurs, le titre de ces deux chapitres du Code de procédure pénale doit également être modifié pour élargir le périmètre initialement dédié aux logiciels de rapprochement judiciaire, en évoquant « l'exploitation judiciaire » des données

[1374] Les deux exceptions notables sont le Système d'Information Schengen (v. *supra* n°705.) et la PNIJ (v. *supra* n°687.). Toutefois ces deux exceptions ne sont pas comparables avec les logiciels de rapprochement judiciaire puisque le SIS s'inscrit dans un environnement numérique d'envergure ayant pour objectif d'échanger des données au niveau européen et la PNIJ est à la fois un traitement et une structure mettant en œuvre les écoutes téléphoniques.
[1375] *Op. cit.* Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.
[1376] V. *supra* n°807.
[1377] Par ex., un site internet, Crim. 20 mai 2015 n°14-81.336 : JurisData n°2015-011834. CONTE Philippe, *Vol d'information,* LexisNexis, Droit pénal n° 10, Octobre 2015, comm. 123.
Autre ex. : un système informatique de données bancaires, Crim. 11 oct. 2016 n°09-88.080.
Ou encore, un ordinateur isolé.
[1378] C. pén. art. 323-1 à 323-8.

recueillies ou générées au cours d'une procédure[1379]. Le projet de décret de l'annexe 3 opère la même modification pour la partie règlementaire[1380].

829. Certains articles du Code de procédure pénale citent les logiciels de rapprochement judiciaire. Ainsi, les articles 230-20 à 230-27 ainsi que R40-39 à R40-41 doivent être modifiés avec en remplaçant le mot « logiciels » par « traitements ». L'expression de « rapprochement judiciaire » doit également être remplacé pour faire référence au TEJ, selon le même principe que pour les titres des chapitres[1381].

830. La nécessité d'étendre la typologie d'informations exploitées. – L'article 230-20 limite le périmètre des investigations qui peuvent être diligentées en précisant que « l'exploitation et le rapprochement » doivent cibler les « informations sur les modes opératoires ». En l'état, les analyses de type fouille de données, telles que celles qui se pratiquent lors de l'exploitation des supports numériques[1382], ne sont donc pas autorisées. Ainsi, actuellement, les enquêteurs habilités ne procèdent pas, en application des dispositions relatives aux logiciels de rapprochement judiciaire, à des analyses de données comme celles qui se pratiquent en expertise ou par le biais d'une réquisition[1383]. Il faut donc proposer d'élargir le cadre général de ces dispositions à de telles analyses, afin qu'il ne soit pas limité aux informations sur les modes opératoires. L'article 230-20 doit être modifié en conséquence[1384].

831. De plus, la notion d'information est trop restrictive. Elle doit être complétée par celle de « données » car, même si la donnée est le support numérique d'une information[1385], l'ajout explicite de la possibilité d'investiguer sur des « données » est important. D'une part, cela rend le traitement d'exploitation judiciaire cohérent avec les autres investigations numériques qui visent explicitement la notion de données (perquisition, réquisition de tiers pour obtenir des informations, etc). D'autre part, cela permet d'exploiter des données purement techniques telles que les métadonnées[1386] ou les

[1379] Annexe 2, proposition de loi, article 1.
[1380] Annexe 3, projet de décret relatif à la mise en œuvre des traitements à des fins d'exploitation et de rapprochement judiciaires, article 8.
[1381] Annexe 2, proposition de loi, articles 2 à 7 et annexe 3, projet de décret relatif à la mise en œuvre des traitements à des fins d'exploitation et de rapprochement judiciaires, articles 9 et 10.
[1382] V. *supra* n°293. et n°807.
[1383] V. *supra* n°300.
[1384] Annexe 2, proposition de loi, article 2.
[1385] V. *supra* n°9.
[1386] V. *supra* n°748.

raw data[1387]. Les modifications correspondantes concernent, non seulement l'article 230-20, mais également l'article R40-40 qui utilise la même terminologie[1388].

832. Une dissociation entre l'obtention des données et leur analyse. – Les actes en procédure pénale se terminent par un rapport ou un procès-verbal qui est versé au dossier[1389]. Le TEJ doit permettre d'analyser toutes les données obtenues au cours d'une procédure, ensemble, mais n'a pas vocation à se substituer aux investigations numériques. Ainsi, par exemple, lorsqu'une captation de données se solde par l'obtention de données, ces dernières seraient désormais appelées à être analysées dans le traitement d'exploitation judiciaire. Il faut donc qu'un rapport soit émis lorsque cette analyse est terminée.

833. Avec la mise en place du traitement d'exploitation judiciaire, une dissociation se créerait entre la récupération ou la génération de données qui continuerait de se faire au travers des investigations numériques, et l'analyse des données obtenues qui se réaliserait postérieurement à la fin de la mesure qui a permis d'obtenir les données. Cette dernière continuerait de se terminer par un procès-verbal, versé à la procédure, accompagné d'un scellé contenant les données obtenues. Conjointement, ces données seraient analysées dans le TEJ qui, pour sa part, dont la mise en œuvre serait autorisée pour toute la durée de la procédure, ce qui résulte de l'article 230-20[1390].

834. Les dispositions des logiciels de rapprochement judiciaire, modifiées pour créer le traitement d'exploitation judiciaire, resteraient conformes avec l'avis de la CNIL rendu au sujet des logiciels de rapprochement judiciaires, qui avait pris acte que « l'utilisation […] ne donne pas lieu à la collecte de nouvelles données à caractère personnel : seules sont utilisées les informations contenues dans les dossiers de procédures, qui ont donc été obtenues dans les conditions prévues par le code de procédure pénale […][1391] ». Cette

[1387] V. *supra* n°9.
[1388] Annexe 2, proposition de loi, article 2 et annexe 3, projet de décret relatif à la mise en œuvre des traitements à des fins d'exploitation et de rapprochement judiciaires, article 9.
[1389] V. *supra* n°757.
[1390] C. pr. pén. art. 230-20 *nouv.* : « Afin de faciliter le rassemblement des preuves des infractions et l'identification de leurs auteurs, les services de la police nationale et de la gendarmerie nationale chargés d'une mission de police judiciaire ainsi que le service placé sous l'autorité du ministre chargé du budget chargé d'effectuer des enquêtes judiciaires peuvent mettre en œuvre, sous le contrôle de l'autorité judiciaire, des traitements destinés à exploiter les données et à faciliter le rapprochement d'informations sur les modes opératoires, réunies par ces services […]. »
[1391] CNIL, Délibération 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).

condition serait vérifiée puisque le TEJ permettrait l'analyse des informations contenues dans la procédure dont font partie les investigations numériques, et n'a pas vocation à collecter de nouvelles données : uniquement d'exploiter celles qui y sont enregistrées.

835. Des rapports itératifs. – La dissociation entre l'obtention des données et leur analyse, aurait une conséquence importante. En effet, le procès-verbal ou le rapport versé à la procédure au terme de d'investigation numérique ayant permis l'obtention des données, ne contiendrait plus le résultat de l'analyse de ces informations. Néanmoins, ces documents resteraient essentiels car ils continueraient de décrire tous les processus relatant l'exécution de l'acte d'obtention des données.

836. Il faut donc que le traitement d'exploitation judiciaire prévoit explicitement que des rapports itératifs et réguliers soient versés au dossier, dès que de nouvelles données ont été introduites dans le traitement et analysées. Actuellement, l'article R40-40 du Code de procédure pénale prévoit bien « l'établissement d'un rapport joint à la procédure », mais uniquement à « la clôture de l'enquête ». Il est donc indispensable de modifier cet article pour prévoir la possibilité de déposer des rapports intermédiaires et itératifs[1392].

837. La fin de l'instabilité des dispositions dues à la décision du Conseil constitutionnel. – Comme précédemment expliqué, la décision du Conseil a laissé les dispositions relatives aux logiciels de rapprochement judiciaire dans un état instable[1393], puisque cette décision a limité le périmètre de cet acte aux informations issues d'une procédure alors que l'esprit du texte était de créer une base de données transversale. Les dispositions issues du texte les ayant créées, n'ont été que très marginalement modifiées postérieurement à la décision du Conseil[1394], laissant ainsi subsister des contradictions entre la conception originelle prévue pour des données transversales et la limitation du rapprochement des informations au sein d'une procédure unique. La proposition de transformer les logiciels de rapprochement judiciaire en traitement d'exploitation

[1392] Annexe 3, projet de décret relatif à la mise en œuvre des traitements à des fins d'exploitation et de rapprochement judiciaires, article 9 : « Des rapports intermédiaires peuvent être établis à tout moment par les agents et militaires habilités, ou à la demande du magistrat ayant autorisé la mise en œuvre du traitement. »

[1393] V. *supra* n°817.

[1394] Seules quelques retouches mineures ont été réalisées postérieurement à la décision du Conseil constitutionnel et ont été introduites, d'une part, par la loi n°2013-1117 du 6 décembre 2013 relative à la lutte contre la fraude fiscale et la grande délinquance économique et financière et, d'autre part, par la loi n°2018-898 du 23 octobre 2018 relative à la lutte contre la fraude. Dans les deux cas, l'objectif est d'étendre utilisation des logiciels de rapprochement judiciaire au service national de douane judiciaire

judiciaire devrait être l'occasion de supprimer ces contradictions. Pour y parvenir, plusieurs modifications seraient nécessaires. Celles-ci sont intégrées dans les propositions de textes des annexes 2 et 3 et commentées ci-après.

838. L'article 230-1, dans son deuxième alinéa, évoque des rapprochements pour des données qui sont « entrées en concordance entre elles ou avec d'autres informations exploitées par le logiciel ». On ne peut que s'interroger sur la provenance des autres informations exploitées par le logiciel dès lors qu'il ne peut y avoir que des informations issues de la procédure en cours. Très clairement, lorsque cet article a été écrit, les autorités publiques pensaient à une base de données transversale[1395]. Cet alinéa devrait donc être supprimé car il nuit à la lisibilité de cet acte.

839. L'article 230-23 est dans le même esprit puisqu'il y ait question de mise à jour des données, « notamment en cas de requalification judiciaire ». Or, dès lors que l'exécution de cette mesure est limitée à une procédure, et que les données exploitées à cette occasion sont, au terme de la procédure, supprimées et mises sous scellés[1396], la mise à jour des données en cours d'enquête est illusoire et, surtout, devient inutile car elle ne peut intervenir que trop tardivement.

840. La rédaction des articles 230-24, 230-27 et R40-41 évoquant le contrôle des mises à jour et les droits d'accès aux informations fait également penser à une base de données nationale et non à un traitement mis en œuvre au sein d'une enquête. Les annexes 2 et 6 proposent de rectifier ces incohérences afin de circonscrire l'exploitation des données réalisées au titre de cet acte, à une procédure.

841. L'article 4 du décret du 7 mai 2012, dont le projet de décret de l'annexe 3 propose l'abrogation et le remplacement[1397], évoque la traçabilité des accès comme s'il s'agissait

---

[1395] V. *supra* n°818.

[1396] L'article R40-40 dans sa nouvelle rédaction qui serait issue du projet de décret (annexe 3, art. 9), prévoirait dans son dernier alinéa, un effacement et une mise sous scellés des données exploitées au cours d'une procédure.

Art. R40-40 *nouv.* : « La mise en œuvre des traitements destinés à exploiter les données et faciliter le rapprochement d'informations mentionnés aux articles 230-20 et suivants est autorisée, pour chaque procédure qu'il contrôle, par le magistrat saisi de l'enquête ou chargé de l'instruction.

En matière d'enquête de flagrance, l'autorisation est réputée acquise sauf décision contraire du procureur de la République.

La mise en œuvre de ces traitements ainsi que l'autorisation du procureur de la République ou de la juridiction d'instruction compétents font l'objet d'une mention en procédure.

A la clôture de l'enquête, les traitements destinés à exploiter les données et à faciliter le rapprochement d'informations mentionnées à l'article 230-20 donnent lieu à l'établissement d'un rapport joint à la procédure. Des rapports intermédiaires peuvent être établis à tout moment par les agents et militaires habilités, ou à la demande du magistrat ayant autorisé la mise en œuvre du traitement. Lors de l'effacement des données prévu l'article 230-22, une copie informatique de l'ensemble des données et informations exploitées est placée sous scellés ou scellés numériques. »

[1397] V. *supra* n°825.

d'un traitement de données transversal. Une telle contradiction est étrange car ce texte, contrairement aux autres dispositions dont la modification vient d'être proposée, a été publié postérieurement à la décision du Conseil constitutionnel. Le projet de décret de l'annexe 3 propose donc d'adapter la traçabilité et l'archivage des données correspondantes à un traitement dont le périmètre se limite à une procédure.

842. Conclusion du sous-paragraphe A : l'adaptation des logiciels de rapprochement judiciaire. – Les investigations numériques conduisent à obtenir des données. L'efficacité de l'exploitation des données ainsi obtenues serait grandement améliorée si elles pouvaient être analysées ensemble, au sein d'un même traitement de données à caractère personnel. C'est la vocation du traitement d'exploitation judicaire dont la création est proposée dans la présente étude. Cette création serait possible en faisant évoluer les dispositions actuelles prévues pour les logiciels de rapprochement judiciaire, qu'une décision du Conseil constitutionnel a bridé par rapport aux objectifs initiaux qui étaient de transposer, par leur intermédiaire, les fichiers d'analyse sérielle à la procédure de droit commun.

843. Néanmoins, pour la mise en œuvre du TEJ, la création de ce dernier ne suffit pas. L'adaptation de certaines investigations numériques doit également être proposée afin que les données obtenues puissent être analysées dans le traitement créé pour une enquête.

B. L'adaptation de l'exploitation des scellés

844. L'alimentation du traitement d'exploitation judiciaire par les autres investigations numériques. – Il est nécessaire de s'assurer que les dispositions relatives aux investigations numériques ne comportent pas de restriction qui ferait obstacle à l'exploitation des données au sein du TEJ[1398]. A l'exception de l'analyse de certains scellés[1399], rien ne s'oppose à ce que les données obtenues par les investigations numériques intrusives alimentent le traitement d'exploitation judiciaire. Cette dissociation entre l'obtention des données et leur analyse[1400] ne soulève aucun problème de légalité.

[1398] V. *supra* n°833.
[1399] V. *infra* n°845.
[1400] V. *supra* n°832.

845. La difficulté de l'alimentation par les données contenues dans certains scellés. – Les données saisies et mises sous scellés lors d'une perquisition[1401] contiennent souvent des informations déterminantes pour la bonne avancée de l'enquête. En revanche, comme précédemment expliqué, leur exploitation est strictement encadrée[1402]. En l'état actuel du droit processuel, les données contenus dans les scellés ne peuvent pas être exploitées dans le cadre du TEJ puisque seule l'ordonnance de commission d'expert autorise l'analyse des scellés en dehors de la présence du mis en examen[1403].

846. La proposition d'une solution prenant en compte les spécificités des données. – Une modification en profondeur de l'article 60-3[1404], étendu en enquête préliminaire[1405] et lors de l'information judiciaire[1406], suffirait à permettre l'intégration des données mises sous scellés lors d'une perquisition dans le TEJ. Pour cela, il est nécessaire de pouvoir s'affranchir de l'intervention des experts pour l'opération de copie des données, qui n'est que l'incarnation d'une méthode palliative utilisant les dispositions inhérentes aux experts pour pouvoir laisser les enquêteurs analyser par eux-mêmes les données[1407]. Pire, le plus gros échec de cette tentative législative, est que les enquêteurs se réquisitionnent entre eux dès qu'ils le peuvent[1408].

847. Il semblerait donc pertinent d'entériner, dans la procédure pénale, une façon de procéder qui, quoi qu'il en soit, fait désormais partie de la pratique quotidienne, en permettant aux enquêteurs spécialisés de réaliser la copie des données précédemment mises sous scellés. Au demeurant, en quoi cette intervention ponctuelle dans la procédure, encadrée dans la mission confiée, d'agents de la Police ou de militaires de la Gendarmerie poserait un problème avéré pour le respect des libertés individuelles ou pour les droits de la défense ? Existerait-il une suspicion envers ces enquêteurs selon laquelle ils pourraient falsifier les données contenues ou introduire frauduleusement des données à charge[1409] ?

[1401] Soit ce sont des supports numériques qui sont saisis tels que des ordinateurs, des clés USB, soit ce sont directement des données (v. *supra* n°249.).
[1402] V. *supra* n°325.
[1403] V. *supra* n°304.
[1404] V. *supra* n°348. L'article 60-3 permet aux enquêteurs de conserver sous leur contrôle l'analyse des données contenues dans un scellé.
[1405] C. pr. pén. art. 77-1-3.
[1406] C. pr. pén. art. 99-5.
[1407] V. *supra* n°349.
[1408] V. *supra* n°350.
[1409] V. *supra* n°330.

Une telle crainte n'a pas plus de sens que d'imaginer que les agents ou militaires des services d'identification judiciaire introduiraient, volontairement, une empreinte ou une trace ADN sur une scène sur laquelle ils interviennent[1410].

848. Le maintien d'une procédure qui assure l'intégrité des données saisies. – Il est toutefois important de conserver l'idée, introduite avec l'article 60-3, d'autoriser une copie des données présentes dans les scellés, et non une analyse directe sur celles-ci. En effet, en cas de contestation ultérieure des résultats des investigations réalisées sur ces données, les magistrats conservent l'entière possibilité de commettre ou de réquisitionner un expert judiciaire civil et indépendant du pouvoir d'enquête[1411], pour procéder à une vérification des résultats énoncés par les enquêteurs.

849. Dans la continuité, afin de prendre toutes les garanties nécessaires à la préservation de l'intégrité des données lors de l'extraction[1412] des données se trouvant à l'intérieur de scellés, il est nécessaire de restreindre les personnes susceptibles de procéder à cette opération. Par cohérence, et dans la continuité de l'esprit de l'exploitation des données numériques consolidées, cette copie doit être confiée aux personnes dont l'habilitation est prévue à l'article 230-25 du Code de procédure pénale[1413]. De plus, pour garantir les droits de la défense au travers de la transparence des opérations réalisées, la traçabilité de ces opérations dans la procédure doit être prévue. Ainsi, la copie des données réalisée en application de l'article 60-3 doit faire l'objet d'une autorisation du procureur de la République, dument inscrite en procédure, et les opérations techniques correspondantes doivent être consignées dans un rapport comportant obligatoirement l'inventaire des scellés[1414].

850. L'extension de l'article 60-3 à l'enquête de flagrance et de l'information judiciaire ne pose pas de difficulté particulière. Dans ce dernier cas, c'est naturellement le Juge d'instruction qui autorise la copie des données. L'ensemble de ces modifications sont

---

[1410] Sur la contestation de l'intégrité du contenu d'un scellé par une partie, v. Crim. 16 avril 2013 n°09-82.944.

[1411] V. *supra* n°344. C. pr. pén. art.230-25 : « Peuvent seuls utiliser les logiciels faisant l'objet du présent chapitre :
1° Les agents des services mentionnés à l'article 230-20, individuellement désignés et spécialement habilités, pour les seuls besoins des enquêtes dont ils sont saisis ; […) »

[1412] Copier, ou encore cloner un support numérique revient à en extraire les données vers un autre support. V. *supra* n°227.

[1413] V. *supra* n°811.

[1414] C. pr.pén. art 60-3 : « […] La personne requise fait mention des opérations effectuées dans un rapport établi conformément aux articles 163 et 166. »

retranscrites dans la proposition de loi visant à améliorer l'efficacité et à renforcer les garanties des traitements de données en procédure pénale[1415].

851. Conclusion du paragraphe §1 : le cadre légal du traitement d'exploitation judiciaire. – Le TEJ pourrait être créé par une évolution des dispositions encadrant les logiciels de rapprochement judiciaire, qui sont actuellement prévues aux article 230-20 du Code de procédure pénale. Une telle évolution permettrait l'analyse conjointe de toutes les données obtenues au travers des investigations numériques intrusives. Pour cela, un traitement de données serait mis en œuvre. Il serait alimenté au fur et à mesure que des investigations numériques sont ordonnées et se terminent.

852. Dans ce contexte, il est nécessaire de s'interroger sur les effets d'une nullité qui viendrait à frapper l'une des investigations numériques ayant contribué à alimenter le TEJ en données.

§2. L'effet des nullités avec le traitement d'exploitation judiciaire

853. L'avantage du cloisonnement des données[1416] dans le cas d'une nullité. – Actuellement, une investigation numérique intrusive[1417] permet, par définition de la notion[1418], l'obtention de données mais, également, dans la majorité des cas, l'exploitation de ces données. C'est le cas avec tous les actes de surveillance[1419], mais aussi avec les actes de fouille[1420], à l'exception de la perquisition. Cette dernière peut conduire à une « simple » saisie de données mises sous scellés, sans qu'elles soient exploitées[1421]. L'analyse fait alors l'objet d'un autre acte[1422]. Dans ce contexte, une éventuelle preuve issue d'une investigation numérique est associée à celle-ci. Dès lors, si cette investigation numérique vient à être annulée, cette preuve est retirée de la procédure ainsi que, les éventuels actes qui découlent directement de celle-ci[1423]. Toutes les preuves

[1415] Annexe 2, proposition de loi, articles 8 et 9.
[1416] V. *supra* n°742.
[1417] V. *supra* n°235.
[1418] V. *supra* n°191.
[1419] V. *supra* n°441.
[1420] V. *supra* n°244.
[1421] La perquisition (v. *supra* n°244.) autorise la fouille des données et donc, leur exploitation, au cours de la perquisition elle-même. Néanmoins, il arrive fréquemment que des objets numériques soient saisis et mis sous scellés, sans qu'ils soient analysés : v. *supra* n°249.
[1422] V. *supra* n°293.
[1423] Sur l'étendue des effets d'une nullité, v. *infra* n°867.

obtenues par les autres investigations numériques ne sont pas affectées par cette nullité, sauf à ce qu'elles fassent partie des actes découlant directement de l'acte annulé.

854. Les risques issus du décloisonnement des données[1424]. – La création d'un traitement d'exploitation judiciaire autoriserait l'analyse, conjointe, des données obtenues par des investigations numériques différentes[1425], puisque celui-ci aurait pour effet de dissocier l'obtention de données au travers d'une investigation numérique et leur exploitation qui se ferait au sein du TEJ[1426]. Le TEJ deviendrait alors un acte d'une importance cruciale au sein d'une enquête. En effet, toutes les éventuelles preuves issues de l'ensemble des investigations numériques intrusives réalisées au cours de l'enquête, proviendraient du TEJ, au travers des rapports itératifs[1427] qui seraient versés à la procédure chaque fois que de nouvelles données seraient introduites dans le traitement. Dès lors, le traitement d'exploitation judiciaire ferait peser sur une procédure un risque important, dans le cas où une nullité serait prononcée, soit pour le TEJ lui-même, soit pour l'une des investigations numériques ayant alimenté celui-ci en données.

855. Il est nécessaire de rappeler le régime des nullités en procédure pénale *(I)* pour pouvoir étudier le risque qui serait induit par la création du TEJ *(II)*.

I – Le régime des nullités en procédure pénale

856. La nécessité de rappeler les principales règles du régime des nullités. – Les présents travaux n'ont pas vocation à entrer dans une étude détaillée du régime des nullités. Pour autant, il est nécessaire de rappeler les éléments principaux permettant de comprendre le risque que pourrait avoir une nullité affectant une investigation numérique, dans le contexte où le traitement d'exploitation judiciaire serait créé. En premier lieu, le régime d'annulation d'un acte est différent suivant qu'une information judiciaire est ouverte ou pas *(A)*. En deuxième lieu, les trois conditions pour qu'une nullité soit recevable doivent être précisées *(B)*. En troisième et dernier lieu, les effets d'une nullité *(C)* sont essentiels pour évaluer et circonscrire les conséquences.

[1424] V. *supra* n°798.
[1425] V. *supra* n°801.
[1426] V. *supra* n°832.
[1427] V. *supra* n°835.

A. La distinction du régime des nullités à l'instruction et devant le tribunal

857. Deux régimes différents. – Il convient de distinguer le cas d'une nullité invoquée lors de l'information judiciaire, de celle qui l'est directement devant le tribunal. En effet, avec la baisse importante de l'ouverture des informations judiciaires[1428], les procédures qui se soldent par la citation directe[1429] d'un prévenu sont, par voie de conséquence, de plus en plus nombreuses.

858. La nullité au stade de l'information judiciaire. – Une requête en nullité peut être déposée devant la chambre de l'instruction « par le juge d'instruction, par le procureur de la République, par les parties ou par le témoin assisté[1430] ». Cette possibilité est ouverte tout au long de l'information judiciaire, et ne s'éteint qu'au travers de l'ordonnance de renvoi qui a pour effet de purger la procédure des éventuelles nullités. Dès lors, en matière délictuelle, le tribunal correctionnel n'est plus compétent pour se prononcer sur des demandes de nullité, sauf si celle-ci concerne l'acte de saisine de la juridiction[1431].

859. La nullité devant le tribunal correctionnel. – S'il n'y a pas d'information judiciaire, autrement dit si le tribunal correctionnel est saisi, notamment par citation directe, la situation est nettement moins encadrée légalement « [puisqu']il n'existe aucun titre spécifique de notre législation afférant aux nullités de l'enquête, qu'elle soit préliminaire ou de fragrance[1432] ». Ainsi, « aucune nullité ne peut être soulevée durant l'enquête[1433] » et c'est le tribunal correctionnel qui est compétent pour statuer sur la nullité de la procédure antérieure. En revanche, les exceptions de nullités doivent être soulevées *in limine litis*, c'est-à-dire avant toute défense au fond[1434].

[1428] V. *supra* n°346.
[1429] C. pr. pén. art. 550. VERNY Edouard, *Procédure pénale*, Dalloz, 6ème édition, p. 222 : « La saisine d'une juridiction sans instruction préparatoire. »
[1430] C. pr. pén. art. 170 et s.
[1431] DREYER Emmanuel et MOUYSSET Olivier, *Procédure pénale,* LGDJ, 2019, p. 400.
[1432] AMBROISE-CASTEROT Coralie et BONFILS Philippe, *Procédure pénale,* puf Thémis droit, 2011 : p. 332 et 333.
[1433] C. pr. pén. art. 385.
Op. cit. p.31. VERGES Etienne, *Procédure pénale* : p. 277.
[1434] DESPORTES Frédéric et LAZERGES-COUSQUER Laurence, *Traité de procédure pénale,* Economica, p.1797.
Sur la sanction de l'irrecevabilité soulevée tardivement :
Crim. 19 sept. 1994 n°93-85.641 : JurisData n°1994-001996, TIXIER Gilbert, *Exceptions de nullité des poursuites — Conditions de recevabilité — Présentation avant toute défense au fond (oui)*, Droit fiscal n° 39, 27 Septembre 1995, comm. 1848.
Crim. 10 dec. 1996 n°96-80.833 : JurisData n°1996-005199.

860. La différence d'égalité des droits de la défense. – Une différence importante apparaît entre les procédures comportant une information judiciaire et celles se soldant par la saisine directe du tribunal. La phase d'instruction préparatoire facilite le respect des droits de la défense, tout particulièrement dans le cas d'investigations numériques intrusives[1435] qui sont des actes fortement attentatoires à la vie privée[1436]. En effet, l'accès au dossier par les parties leur permet d'avoir régulièrement connaissance des éléments à charge. Il y a là une condition importante du respect des droits de la défense[1437]. Ainsi, dans le cas d'une investigation numérique, une partie dispose de temps pour prendre connaissance du procès-verbal ou du rapport versé à la procédure et, le cas échéant, déposer une requête en nullité. Lors d'une saisine directe du tribunal, les parties, d'une part, disposent de moins de temps et, d'autre part, reçoivent l'intégralité du dossier en fin de procédure ce qui en rend la compréhension nettement plus délicate.

861. Cette différence de régime, fonction de la procédure mise en œuvre pour la mise en état du dossier d'enquête, se ressent particulièrement dans le cas des investigations numériques, en raison de l'intrusion forte dans la vie privée. Ces dernières sont également directement concernées par les conditions de recevabilité d'une nullité, notamment avec la notion de « qualité à agir ».

B. Les conditions de recevabilité d'une action en nullité

862. Les trois critères cumulatifs. – Lorsqu'une juridiction est saisie d'une action en nullité contre un acte de procédure, elle doit étudier trois questions pour se prononcer sur la recevabilité. « Une réponse négative à l'une des questions dispense d'examiner la question suivante[1438] ».

863. En premier lieu, le juge doit s'interroger si le requérant a intérêt à demander l'annulation de l'acte. Cette condition est très proche de l'absence de grief[1439], mais elle n'en a pas le même objet. L'intérêt pour agir renvoie à la condition de recevabilité de la demande. Ainsi, la Cour de cassation a confirmé que le Parquet avait intérêt à agir en raison du « droit absolu et général [conféré au ministère public pour] interjeter appel de toutes les ordonnances du juge d'instruction ou du juge des libertés et de la détention,

---

[1435] V. *supra* n°235.
[1436] Dans le contexte de numérisation de notre société (v. *supra* n°17.), les objets numériques sont des supports très importants de la vie privée.
[1437] Sur l'application de l'article 6 de la Convention européenne des droits de l'Homme, v. *supra* n°313.
[1438] *Ibid*. DESPORTES Frédéric et LAZERGES-COUSQUER Laurence, *Traité de procédure pénale,* p.1245.
[1439] V. *infra* n°865.

même celles conformes à ses réquisitions[1440] ». Cet arrêt confirme que « l'intérêt à agir », se réfère au droit de pouvoir engager une action en nullité. Les investigations numériques ne présentent pas de spécificités particulières par rapport aux autres actes d'enquête sur l'intérêt à agir, à la différence de la deuxième question que doit se poser le juge.

864. En deuxième lieu, la qualité pour agir est une autre condition, mais qui est composée de deux éléments. Tout d'abord, la personne invoquant la nullité doit avoir la qualité de partie ou de témoin assisté, même si cette condition a été assouplie par la jurisprudence. En effet, une nullité relative à une pièce issue d'une autre procédure peut être soulevée par une partie qui n'était pas partie dans le dossier dont est issue la pièce[1441]. Cette extension du contrôle aux actes issus d'une autre procédure concerne tout particulièrement les investigations numériques, notamment les écoutes téléphoniques[1442]. Ensuite, pour qu'une personne ait la qualité pour agir, la violation invoquée doit avoir pour objet de préserver ses droits et ses libertés[1443]. Les écoutes téléphoniques sont ici, également, concernées. En effet, la Cour de cassation considérait que seul le titulaire de la ligne écoutée était bienfondé à demander l'annulation de l'acte[1444], jusqu'à ce que la France soit condamnée par la CEDH[1445]. Depuis, un revirement de jurisprudence autorise les tiers écoutés à agir[1446].

865. En troisième lieu, l'existence d'un grief pour la partie invoquant la nullité, est également un critère obligatoire. « Le grief est le préjudice causé par l'irrégularité à la partie concernée[1447] ». L'exigence d'un grief est une condition appliquée avec beaucoup de rigueur par la Cour de cassation, qui provient essentiellement du fait que les nullités textuelles sont rares, notamment dans le cas des investigations numériques. Lorsque de telles nullités existent, elles concernent souvent le détournement de procédure[1448]. Dès

---

[1440] Crim. 30 sept. 2014 n°14-84.834 : JurisData n°2014-022705.
[1441] Crim. 19 dec. 2007 n°07-86.885 : JurisData n°2007-042162.
Crim. 16 fév. 2011 n°10-82.865 : JurisData n°2011-003741.
[1442] *Ibid.*
[1443] Droit à un procès équitable, droits de la défense, droit à la vie privée, etc.
[1444] Crim. 10 mars 1993 n°91-80.936 : JurisData n°1993-704828.
[1445] CEDH 24 août 1998 Lambert c. France.
[1446] Crim. 15 janv 2003 n°02-87.341 : JurisData n°2003-017563 – BUISSON Jacques, *L'intérêt à agir de l'auteur d'une requête en annulation doit permettre un contrôle efficace des actes d'administration de la preuve*, LexisNexis Procédures n° 5, Mai 2003, comm. 121.
CAPDEPON Yannick, *Ecoutes judiciaires – La nullité d'une écoute téléphonique sur la ligne d'un tiers,* LexisNexis, Droit pénal n°12, décembre 2017.
[1447] *Ibid*. DESPORTES Frédéric et LAZERGES-COUSQUER Laurence, *Traité de procédure pénale,* p.1237.
[1448] V. par ex. C. pr. pén. art. 706-95-14 al.4 : « Les opérations ne peuvent, à peine de nullité, avoir un autre objet que la recherche et la constatation des infractions visées dans les décisions du magistrat. »

lors, ce sont les nullités substantielles qui sont les plus fréquemment soulevées et pour lesquelles la rigueur de la Cour s'exprime avec fermeté[1449]. En effet, pour que la nullité de l'acte soit retenue, une atteinte directement portée à un droit du requérant[1450] doit exister. Ainsi, même si l'existence de la nullité est reconnue, mais si, par exemple, la méconnaissance des prescriptions légales a été compensée par des conditions suffisantes à celles exprimées par le texte, le grief n'existe pas selon la Cour[1451]. De même, la Cour retient que si une partie ou son avocat était présent lors de l'accomplissement de l'acte irrégulier et n'a soulevé aucune protestation, il s'agit d'une forme de renonciation implicite[1452].

866. Un filtre important. – Les trois critères qui viennent d'être précisés, appliqués cumulativement par la Cour de cassation, contribuent à écarter beaucoup de nullités. Pour autant, dans le contexte de création d'un traitement d'exploitation judiciaire, il est essentiel de rappeler les effets d'une nullité lorsque celle-ci est retenue par le juge. En effet, les éventuelles preuves issues de l'analyse des données conjointes provenant de plusieurs investigations numériques, deviendraient hautement critiques pour une procédure si une nullité venait à frapper l'une de ces investigations ou l'acte autorisant la mise en œuvre le TEJ.

C. Les effets d'une nullité

867. Les deux effets d'une nullité. – Il convient de distinguer les effets d'une nullité sur les procédures *(1)* de l'étendue de l'annulation aux actes *(2)*.

1. Les effets sur les procédures

868. L'effet général de la nullité au sein de la procédure. – Lorsqu'une pièce est annulée, cette annulation est opposable à toutes les parties à la procédure. Ainsi, si seule une partie est à l'origine de l'action en nullité et qu'elle ait gain de cause, la nullité devient

Sur le détournement de procédure : FOURMENT François, *Détournement de procédure, fraude au champ d'application d'un pouvoir d'enquête ou d'instruction,* LexisNexis, Droit pénal n°9, septembre 2019, comm. 156.

[1449] FOURMENT François, *Nullités de l'instruction : un exemple de grief !* Gazette du Palais, 19 juillet 2016, n°271bO, p.68.

[1450] Crim.10 mai 2016 n°15-87.713, Bull. crim. 2016, n°850. Dalloz actualité, 25 mai 2016, obs. AUBERT D.

[1451] Crim. 7 juin 1988 n°88-81.828, Bull. crim. 1988 n°258.

[1452] Crim. 11 janv. 1994 n°93-84.837, Bull. crim. 1994 n°15.

opposable aux autres parties, même si ces dernières ne l'avaient pas demandée, voire même l'avaient contestée.

869. L'effet conditionnel de la nullité au sein des autres procédures. – En revanche, l'annulation ne concerne, en principe, que la procédure au sein de laquelle elle est prononcée, et ne remet pas en cause la validité de la pièce dans les autres procédures où elle a été versée[1453]. Néanmoins, il est dérogé à cette règle lorsque le versement de la pièce dans l'autre procédure a eu lieu avant l'annulation[1454] ou si, lorsque la pièce en question a été versée postérieurement, elle constitue le fondement des nouvelles poursuites[1455]. Dans ce dernier cas, on parle de procédure incidente[1456]. Les effets de l'annulation d'un acte sur une autre procédure sont importants pour l'étude de la mise en œuvre du traitement d'exploitation judiciaire, car les investigations numériques peuvent souvent révéler des comportements répréhensibles différents de ceux à l'origine de l'acte originel[1457].

2. Les effets sur les actes

870. L'étendue de l'annulation quant aux actes. – Il s'agit d'un point essentiel pour l'étude des risques potentiels qu'introduirait la création d'un traitement d'exploitation judiciaire. En effet, ce dernier aurait pour effet d'analyser, ensemble, toutes les données obtenues au travers de toutes les investigations numériques réalisées au sein d'une procédure[1458]. Dès lors, il est important de cerner l'étendue qu'aurait l'annulation de l'une de ces investigations numériques ou de l'acte mettant en œuvre le TEJ.

871. Il convient de distinguer le sort des actes frappés d'irrégularités, des effets que l'annulation peut avoir sur d'autres actes.

872. Le sort des actes entachés d'irrégularités. – L'acte atteint de nullité peut être annulé totalement ou partiellement. Lorsque l'annulation est totale, l'acte annulé est réputé n'avoir jamais existé de sorte que les parties ne peuvent plus en évoquer les

[1453] Crim. 9 mars 1981 n°80-93.646, Bull crim. 1981 n°86.
Crim. 16 fev. 2000 n°99-86.307, Bull. crim. 2000 n°72.
[1454] Crim 27 fev. 2001 n°00-86.747, Bull. crim. 2001 n°50.
[1455] Crim. 27 mars 1995 n° 94-85.074, Bull. crim. 1995 n°127.
[1456] CAMOUS Eric, *Les procédures incidentes : le point de vue d'un magistrat du parquet,* Gazette du Palais, 19 juillet 2016, n°271a5, p.70.
[1457] V. notamment l'enquête sous pseudonyme, v. *supra* n°474.
[1458] V. *supra* n°801.

résultats. Si l'acte n'est annulé que partiellement, seuls les fragments annulés sont retirés de la procédure. Ainsi, un procès-verbal est biffé pour que les éléments annulés ne puissent plus être invoqués[1459]. Le reste des éléments reste valable.

873. L'annulation des actes subséquents. – L'acte annulé peut entraîner l'annulation d'autres actes au sein de la procédure. C'est au juge qu'il appartient d'apprécier l'étendue de l'annulation[1460]. Il peut le faire, soit à la demande des parties, soit d'office[1461]. La Cour de cassation énonce, au visa des articles 174 et 802 du Code de procédure pénale, que « lorsqu'une irrégularité constitue une cause de nullité de la procédure, seuls doivent être annulés les actes affectés par cette irrégularité et ceux dont ils sont le support nécessaire[1462] ». Néanmoins, l'annulation doit être étendue à tous les actes qui découlent directement de l'acte annulé[1463]. C'est cette règle qui prend une importance cruciale pour l'étude des risques liés à la mise en œuvre d'un TEJ au sein d'une procédure[1464].

874. Conclusion du sous-paragraphe I : le régime des nullités en procédure pénale. – Les éléments principaux relatifs au régime des nullités fournissent un éclairage essentiel pour parvenir à étudier les risques qu'introduirait la création d'un traitement d'exploitation judiciaire. Ce sont, tout particulièrement, la notion de qualité à agir, jusque-là fortement associée aux écoutes téléphoniques, ou encore les effets d'une annulation sur les actes subséquents, qui constituent la base de l'étude des risques des effets d'une nullité dans le contexte du TEJ.

II – Le risque des effets d'une nullité dans le contexte du TEJ

875. Les deux risques liés aux nullités avec la création d'un TEJ. – Le traitement d'exploitation judiciaire aurait pour effet de permettre l'analyse, ensemble, de toutes les données obtenues par les investigations numériques diligentées au sein d'une procédure. Dans ce contexte, il y aurait, potentiellement, une importante concentration des preuves qui pourraient être issues du TEJ. En effet, actuellement, l'exploitation des données est

[1459] Dans ce cas, on parle de cancellation des pièces.
DUMONT Jean, GEORGET Valérie et BONNET Audrey, *Fasc. 20 : Les nullités de l'information,* JurisClasseur Procédure pénale.
[1460] C. pr. pén. art. 174 al. 2.
[1461] Crim. 1er déc. 1987 n°87-85.270 : JurisData n°987-002030.
[1462] Crim. 3 avr. 2007 n°06-87.264 : JurisData n°2007-038631.
[1463] Crim. 10 déc. 1968 n°68-92.02, Bull. crim. 1968 n°333.
[1464] V. *infra* n°887.

principalement réalisée au sein des actes d'investigations numériques permettant leur obtention[1465]. Ainsi, si l'une d'entre elles vient à être annulée, seules les éventuelles preuves issues de cette investigation numérique risquent d'être retirées de la procédure, nonobstant les éventuels actes qui en découleraient directement[1466]. Avec le TEJ, le risque est fortement accru puisque le fait d'alimenter ce traitement en données au fur et à mesure que des investigations numériques sont réalisées[1467], rend en quelque sorte les données solidaires les unes des autres. Or, en cas de nullité de l'un des actes ayant contribué à alimenter le traitement, le risque que l'annulation de l'analyse de toutes les données ainsi regroupées soit soulevée, est dangereux et doit donc être identifié et maîtrisé.

876. Pour cela, il est nécessaire d'étudier l'annulation du TEJ lui-même *(A)*, et l'annulation de l'une des investigations numériques ayant alimenté en données le TEJ *(B)*.

A. Les effets de l'annulation du TEJ

877. La possibilité d'une action en nullité dirigée vers le TEJ. – La proposition de créer le traitement d'exploitation judiciaire repose sur une évolution des logiciels de rapprochement judiciaire[1468]. Le TEJ serait donc un acte d'enquête. A ce titre, une partie pourrait agir en nullité contre les conditions de sa mise en œuvre ou de son exécution, en application du cadre général du régime des nullités[1469]. Par exemple, un défaut de l'autorisation ou un non-respect du formalisme de la mise en œuvre du TEJ[1470] au sein d'une procédure pourrait être à l'origine d'une action en nullité. Aucune jurisprudence n'est retrouvée pour une telle action envers les logiciels de rapprochement judiciaire dont serait issu le traitement d'exploitation judiciaire mais, d'une manière générale, dans le cas des investigations numériques, la Cour de cassation est très stricte quant au respect des formalités inhérentes à leur mise en œuvre. Dans le cas de la géolocalisation[1471], le

[1465] V. *supra* n°755.
[1466] V. *supra* n°873.
[1467] V. *supra* n°832.
[1468] V. *supra* n°803.
[1469] V. *supra* n°862.
[1470] C. pr. pén. art. R40-40 *nouv.* : « La mise en œuvre des traitements destinés à exploiter les données et faciliter le rapprochement d'informations mentionnés aux articles 230-20 et suivants est autorisée, pour chaque procédure qu'il contrôle, par le magistrat saisi de l'enquête ou chargé de l'instruction.
[…]
La mise en œuvre de ces traitements ainsi que l'autorisation du procureur de la République ou de la juridiction d'instruction compétents font l'objet d'une mention en procédure. »
[1471] C. pr. pén. art. 230-32 et s. Pour l'étude détaillé de la mesure, v. *supra* n°486.

manque de rigueur du juge d'instruction dans les autorisations nécessaires[1472] entraîne systématiquement la nullité de la mesure[1473]. Procédant de la même logique, une irrégularité de l'autorisation de mise en œuvre du TEJ au sein d'une procédure pourrait motiver une action en nullité.

878. Les effets de l'annulation du TEJ. – Dans l'hypothèse où l'annulation serait prononcée, soit l'acte est annulé dans sa totalité, soit il peut l'être partiellement[1474]. Dans ce second cas, il faut que le juge soit en capacité de se prononcer sur ce qui doit être retiré de la procédure au sein de l'acte frappé d'irrégularité. Le TEJ doit donc mettre à disposition du juge des éléments lui permettant de procéder à ce tri. Cette situation est identique à l'annulation d'une investigation numérique ayant alimenté en données le TEJ, puisque le juge doit pouvoir déterminer quelles preuves découlent de la mesure annulée. Ce point fait l'objet de développements spécifiques[1475]. Seul le cas de l'annulation du TEJ dans sa totalité est étudié ici.

879. L'annulation du TEJ dans sa totalité, tout particulièrement si celle-ci intervient en fin de procédure ou dans le cas où elle serait prononcée par le tribunal correctionnel[1476], introduirait un risque important pour le dossier, puisque c'est potentiellement un nombre important de preuves qui pourraient être retirées[1477].

880. La nécessaire maîtrise du risque d'annulation du TEJ. – Aucune donnée ne serait directement obtenue au travers du traitement d'exploitation judiciaire. En effet, la création de celui-ci aurait pour effet de dissocier l'obtention des données de leur exploitation[1478]. Le rôle du TEJ se limiterait à permettre l'analyse des données qui seraient obtenues au travers des investigations numériques intrusives[1479]. En conséquence, l'annulation du TEJ n'entraînerait la perte d'aucune donnée obtenue par une investigation.

[1472] Dans le cas de la géolocalisation, plusieurs autorisations sont prévues par les textes : v. *supra* n°494.
[1473] Crim. 20 Juin 2018 n°17-86.657 : JurisData n°2018-010675. CLEMENT Eloi, *Précisions sur la régularité de la procédure*, Dalloz, AJ Pénal, AJ pénal 2018, p. 474.
Crim. 25 Juillet 2018 n°18-80.651 : JurisData n°2018-014001. Obs. *Géolocalisation (validité) : substitution de motivation par la chambre de l'instruction*, Recueil Dalloz 2018, p. 1649.
[1474] V. *supra* n°872.
[1475] V. *infra* n°887.
[1476] V. *supra* n°859.
[1477] Toutes les preuves issues des investigations numériques : v. *supra* n°875.
[1478] V. *supra* n°832.
[1479] V. *supra* n°235.

881. De plus, toujours grâce à la dissociation entre l'obtention des données et leur analyse, les informations numériques obtenues au travers d'une investigation sont systématiquement mises sous scellés à la fin de l'acte, et sont jointes au procès-verbal ou au rapport[1480]. Puisque l'exploitation des données obtenues est réalisée au sein du TEJ, ce sont en quelque sorte des données « brutes », qui seraient mises sous scellés à la fin d'une investigation numérique. En cas d'annulation de l'acte ayant mis en œuvre le traitement d'exploitation judiciaire, et donc des preuves qui en auraient été déduites, le juge conserverait la possibilité d'ordonner une analyse des données saisies et mises sous scellés lors de l'investigation numérique[1481]. Dans le cas des données mises sous scellé lors d'une perquisition, le cadre légal proposé pour créer le TEJ prévoit que c'est une copie des informations numériques qui est enregistrée dans le traitement[1482]. Les données d'origines resteraient ainsi protégées.

882. Certes, la méthode pour pallier l'annulation du TEJ qui consisterait à ordonner une nouvelle exploitation des données initialement obtenues lors de l'investigation numérique, aurait pour conséquence d'allonger les délais de la procédure, mais elle permettrait de pouvoir retrouver des preuves issues du TEJ et retirées du dossier. Cette possibilité de pouvoir reverser au dossier une preuve annulée est très importante pour la stabilité de la procédure puisque, outre la preuve en elle-même qui peut s'avérer déterminante pour le procès, elle peut limiter les effets de l'annulation du TEJ. En effet, la Cour de cassation doit annuler tous les actes subséquents, c'est-à-dire directement liés à l'acte annulé[1483], en l'occurrence le TEJ. Or, le fait de pouvoir retrouver un élément qui a orienté l'enquête, déclenchant de nouvelles investigations qui n'auraient pas existées sans l'élément annulé, permettrait de limiter les effets de l'annulation du TEJ. Par exemple, si une géolocalisation a aiguillé les enquêteurs vers un individu, inconnu de la procédure jusque-là, et que cette personne ait été mise en garde à vue suite à la géolocalisation, les procès-verbaux des auditions doivent être annulés si la géolocalisation est précédemment déclarée irrégulière[1484].

883. Le fait de pouvoir retrouver, par le biais d'une exploitation directe des données mises sous scellés au terme de la mesure de géolocalisation, permettrait à la chambre

[1480] Sur le déroulement d'une investigation numérique, v. *supra* n°758.
[1481] Selon les actes autorisant la fouille des scellés numériques : v. *supra* n°293.
[1482] V. *supra* n°848.
[1483] V. *supra* n°873.
[1484] Crim. 28 nov. 2001, n°01-86.467 : JurisData n° 2001-012269. La cour a censuré un arrêt d'une chambre d'instruction qui avait refusé d'annuler des procès-verbaux d'audition qui trouvaient leur source dans une audition annulée.

d'instruction ou au tribunal de ne pas annuler les actes qui découlent de l'exploitation de ces données.

884. La perte potentielle de certaines preuves. – Néanmoins, malgré cette solution qui permettrait de récupérer les preuves retirées de la procédure suite à l'annulation du TEJ, il subsiste un risque résiduel de perdre certaines preuves, intrinsèques à la raison justifiant l'analyse toutes les données obtenues au sein d'une enquête, ensemble[1485]. En effet, la proposition de créer le traitement d'exploitation judiciaire trouve sa source dans l'évolution des techniques informatiques qui pourrait améliorer l'efficacité de l'exploitation des données, en les analysant ensemble plutôt que cloisonnées acte par acte[1486]. Ainsi, dans l'hypothèse où le TEJ permettrait d'obtenir des preuves grâce à la corrélation qu'il établit entre des données issues d'investigations numériques différentes, ces éléments seraient définitivement perdus pour la procédure suite à l'annulation du TEJ, puisqu'ils ne pourraient pas être récupérés par l'analyse des données isolément.

885. Conclusion du sous-paragraphe A : les effets de l'annulation du TEJ. – Le traitement d'exploitation judiciaire aurait vocation à regrouper toutes les données obtenues au travers des investigations numériques, afin d'améliorer leur exploitation. Il en découle un risque important dans le cas où le TEJ serait annulé, puisqu'il concentrerait toutes les preuves issues des investigations numériques. La dissociation entre l'obtention des données et leur analyse offrirait au juge, dans le cas où une nullité frapperait le TEJ, d'ordonner une fouille des scellés contentant les informations obtenues au terme d'une investigation numérique. Cette possibilité limiterait considérablement le risque de perdre des preuves en raison de la mise en œuvre d'un TEJ. Néanmoins, un risque résiduel subsiste pour les preuves qui seraient le fruit de la corrélation des différentes données analysées conjointement au sein de ce traitement.

886. De plus, un autre risque doit être étudié, puisque le cas où une nullité serait prononcée à l'encontre de l'une des investigations numériques ayant alimenté en données le TEJ, pourrait avoir également de lourdes conséquences.

[1485] V. *supra* n°739.
[1486] V. *supra* n°764.

B. Les effets de l'annulation d'un acte ayant alimenté en données le TEJ

887. La possibilité d'une action en nullité envers une investigation numérique ayant alimenté le TEJ en données. – Une action en nullité contre une investigation numérique ayant alimenté en données le traitement d'exploitation judiciaire est un incident de procédure fortement probable. En effet, en premier lieu, ces actes sont potentiellement nombreux au cours d'une enquête[1487]. En second lieu, ils sont des actes intrusifs. A ce titre, la licéité de leur exécution fait fréquemment l'objet de contestations[1488].

888. Le risque dû aux effets de la nullité d'une investigation numérique sur le TEJ. – Si la nullité d'une investigation numérique ayant alimenté en données le TEJ est prononcée, le juge doit analyser les conséquences sur les autres actes de la procédure pour, le cas échéant, annuler les éléments qui découlent directement de l'acte déclaré irrégulier[1489]. Avec le TEJ, l'annulation d'une investigation numérique aurait pour conséquence que les données obtenues au travers de cet acte soient retirées de la procédure, et donc du traitement d'exploitation judiciaire.

889. Or, cette nécessité de retirer les données du TEJ devient complexe en raison de la temporalité d'une procédure pénale. En effet, les délais de communication des pièces[1490], ou si un prévenu est directement renvoyé devant le tribunal correctionnel[1491], la nullité de l'acte en question serait prononcée alors que de nombreuses autres investigations numériques auraient été exécutées. Par voie de conséquence, les données de l'acte annulé auraient déjà été utilisées au sein du TEJ, associées aux autres informations numériques, pour obtenir d'éventuelles preuves.

890. Par exemple, une enquête, au sein de laquelle trois investigations numériques « A », « B » et « C » sont exécutées, peut être prise en exemple. Lorsque ces actes se terminent, un procès-verbal est versé à la procédure et des données sont mises sous scellés[1492]. Conjointement elles alimentent le TEJ afin d'être analysées ensemble.

[1487] Par ex. l'analyse d'un ordinateur, une captation de données, une enquête sous pseudonyme, etc.

[1488] V. par ex, les contestations récentes d'interception de correspondances : Crim. 24 sept. 2019, n°18-85.736 : JurisData n°2019-016683 ; Crim. 16 janv. 2019, n°18-86.127.
Ou les contestations d'une mesure de géolocalisation : Crim. 18 sept. 2019, n°18-84.752 ; Crim. 3 sept. 2019, n°19-80.164.

[1489] V. *supra* n°873.

[1490] Lors de l'information judiciaire, même si le juge d'instruction notifie régulièrement aux parties les résultats des investigations, il y a un délai : v. *supra* n°860.

[1491] V. *supra* n°859.

[1492] V. *supra* n°833.

L'analyse des données issues de ces trois actes peut révéler des preuves. Si une partie demande l'annulation de l'acte « A », et qu'elle obtienne gain de cause, que deviennent alors les preuves numériques obtenues ?

891. La nécessaire maîtrise du risque d'annulation d'une investigation numérique ayant alimenté TEJ. – L'exemple précédent révèle la nécessité, pour le traitement d'exploitation judiciaire, d'établir et de conserver un historique efficace des données effectivement exploitées pour obtenir une preuve. En effet, si l'acte « A » est annulé, il est évident que tous les résultats obtenus au travers de l'analyse des données de « A », ou avec « A », doivent être annulés. Le nouveau risque qui serait introduit avec la création d'un TEJ, concernerait précisément le deuxième cas de figure, c'est-à-dire les preuves obtenues par l'exploitation de données mélangées avec celles issues de l'acte « A ».

892. La nécessité de pouvoir séparer les résultats obtenus. – Le TEJ doit donc pouvoir permettre de trier les données issues des différentes investigations numériques lorsqu'elles sont exploitées, afin que, dans l'exemple précédent, les éléments issus de l'analyse des données obtenues avec les investigations « B » et « C », ne soient pas affectés par l'annulation de l'acte « A ». En effet, lorsque la chambre de l'instruction ou le tribunal correctionnel prononce la nullité de l'acte « A » et qu'il doit étudier les effets de cette irrégularité sur le reste de la procédure, il doit pouvoir disposer d'éléments lui permettant d'apprécier quelles sont les preuves déduites du TEJ auxquelles les données de « A » ont contribué.

893. La nécessité d'associer le droit et la technique. – Pour parvenir à cela, le TEJ doit mettre en œuvre une traçabilité et un historique de l'exploitation des données réalisée. Une telle mise en œuvre nécessite que le cadre légal s'intéresse aux outils techniques utilisés pour le TEJ. Ce lien avec la technique ne serait pas nouveau puisqu'il existe des précédents où des textes règlementaires font directement référence à un cahier des charges techniques. C'est notamment le cas avec les décrets de création des logiciels de

rapprochement judiciaire[1493] et des fichiers d'analyse sérielle[1494] qui renvoient à des dossiers techniques de présentation de ces outils.

894. Partant du même raisonnement, il est essentiel que le projet de décret relatif à la mise en œuvre du TEJ[1495] impose une fine granularité dans l'historique de l'utilisation des données enregistrées dans le traitement, ce qui est concrétisé au travers de la proposition d'article 7 de ce texte[1496]. Cette contrainte de traçabilité permettant d'enregistrer toutes les actions effectuées au sein du traitement devrait donc être prise en compte dans la mise en œuvre technique du TEJ. Ce point fait l'objet de développements spécifiques[1497].

895. Conclusion de la section 1 : le regroupement des données par la création du « traitement d'exploitation judiciaire ». – La proposition de créer le traitement d'exploitation judiciaire a pour objectif de permettre l'analyse conjointe de toutes les données obtenues au travers des investigations numériques intrusives, au sein d'une procédure. La création du TEJ pourrait être réalisée au travers d'une évolution des dispositions encadrant actuellement les logiciels de rapprochement judiciaire, qui serait réalisée grâce à deux textes : une proposition de loi et un projet de décret. Cependant, la création légale et règlementaire du TEJ génère un nouveau risque important pour les procédures pénales, qui trouverait sa source dans la nullité du TEJ lui-même ou dans celle d'une investigation numérique qui aurait contribué à fournir des données au TEJ. En effet, en raison de son objectif, le traitement d'exploitation judiciaire serait potentiellement à l'origine d'un nombre important de preuves versées au dossier. Dès lors, son annulation pourrait vider une procédure de ses éléments principaux. Ce risque est maîtrisé par une séparation de l'obtention des données au travers des investigations numériques et de leur analyse au sein du TEJ. Si ce dernier venait à être annulé, le juge pourrait ordonner une exploitation « classique[1498] » des données mise sous scellés au terme de l'investigation numérique.

[1493] Décret n°2012-687 du 7 mai 2012 relatif à la mise en œuvre de logiciels de rapprochement judiciaire à des fins d'analyse criminelle. V. *supra* n°719.
[1494] 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 ». *Ibid.*
[1495] V. *supra* n°825.
[1496] V. annexe 3, projet de décret, article 7 : « Cette infrastructure doit notamment permettre d'établir la provenance des données introduites dans un traitement mis en œuvre au titre des présentes, et permettre la traçabilité complète des corrélations entre les résultats obtenus et la provenance des données introduites. »
[1497] V. *infra* n°914.
[1498] V. *supra* n°293.

896. De plus, pour que la proposition de créer un TEJ soit réaliste, le cadre légal et la maîtrise des risques quant à son annulation ne sont pas suffisant. La mise en œuvre concrète du traitement d'exploitation judiciaire doit également reposer sur des éléments réalistes et réalisables.

Section 2. La mise en œuvre du « traitement d'exploitation judiciaire »

897. La nécessité d'une mise en œuvre crédible. – La possibilité de pouvoir analyser, ensemble, toutes les données obtenues au cours d'une enquête, constituerait une amélioration importante de l'efficacité des investigations numériques en enquête pénale. La proposition de créer un traitement d'exploitation judiciaire (ci-après « TEJ ») est une réponse à cette nécessité. Pour ce faire, la présente étude montre qu'un cadre légal et règlementaire pourrait permettre une telle création, sans chamboulement de la procédure pénale. Pour autant, pour que le TEJ soit un acte réaliste, la possibilité de créer un cadre légal et réglementaire n'est pas suffisante. En effet, un tel acte doit également être crédible dans sa mise en œuvre au sein des enquêtes. Une mesure qui supposerait un investissement informatique démesuré pour chaque gendarmerie et commissariat du territoire, ou qui nécessiterait un chamboulement total de l'organisation des enquêteurs spécialisés en criminalité informatique[1499] au sein des force de l'ordre, serait totalement irréaliste. Par exemple, si tous les enquêteurs spécialisés devaient être titulaires d'un diplôme d'ingénieur ou d'un doctorat en informatique pour être capable d'utiliser le TEJ, la mise en œuvre organisationnelle[1500] du TEJ anéantirait la proposition d'analyser, ensemble, les données obtenues au sein d'une enquête, par ce biais-là.

898. Un acte qui doit pouvoir concerner toutes les enquêtes. – Le respect d'une mise en œuvre crédible est essentielle pour que le TEJ puisse être utilisé dans toutes les procédures. Il ne doit pas être réservé à des enquêtes de grande criminalité ou fortement médiatisées[1501] en raison d'un coût exorbitant.

899. L'étude de la mise en œuvre. – La présente étude n'a pas pour ambition de fournir une réponse technique parfaitement aboutie, mais de démontrer que la proposition

[1499] V. *supra* n°323.
[1500] Dictionnaire Larousse : « Qui concerne l'organisation d'un groupe, d'une entreprise, etc. »
[1501] V. *supra* n°339.

d'un cadre légal et règlementaire créant un TEJ n'est pas qu'une étude juridique théorique, et est possible en raison d'une mise en œuvre crédible.
Pour étudier cette faisabilité, les aspects techniques de la mise en œuvre du TEJ *(§1)* et les aspects organisationnels *(§2)* sont distingués.

§1. La mise en œuvre technique du TEJ

900. Une mise en œuvre technique crédible. – Le cadre légal et réglementaire proposé[1502] pour créer le traitement d'exploitation judiciaire impose tacitement un certain nombre de contraintes informatiques. Pour que la mise en œuvre du TEJ soit faisable, ces contraintes ne doivent pas nécessiter un cadre technique irréaliste, c'est-à-dire imposant, notamment, des investissements démesurés. Pour étudier cette mise en œuvre technique, l'environnement informatique permettant d'accomplir les analyses de données consolidées, doit être simple et le plus proche possible de ce qui existe actuellement.
De manière classique, l'infrastructure matérielle[1503] *(I)* et les logiciels *(II)* sont étudiés séparément.

I – La mise en œuvre de l'infrastructure physique

901. L'expérience d'une dérive des coûts. – La PNIJ[1504] constitue un exemple de création d'une infrastructure informatique au service de l'enquête pénale. Malgré un suivi rigoureux des services de l'état, la dérive des coûts de mise en œuvre et d'exploitation reste dans les mémoires. Au demeurant, même si certaines difficultés lors de la création de la plateforme ont contribué à dépasser le budget initial, la dérive des coûts est principalement due aux besoins en rétention de données[1505] qui augmentent régulièrement, essentiellement en raison du contexte terroriste.

902. Un danger exponentiel avec le traitement d'exploitation judiciaire. – Or, la PNIJ est une plateforme nationale et donc unique[1506]. Avec le déploiement

[1502] V. *supra* n°800.
[1503] Communément désigné sous le nom de « *hardware* ».
[1504] La PNIJ est la structure compétente pour centraliser les demandes d'écoutes téléphoniques. Elle se positionne à l'interface entre les autorités judiciaires et les opérateurs de téléphonie. V. *supra* n°687.
[1505] Notamment au titre des « prestations annexes », qui concernent la rétention de toutes les données qui transitent par la ligne écoutée : v. *supra* n°543.
[1506] C. pr. pén. art. 230-45 : « […] Sauf impossibilité technique, les réquisitions et demandes […] sont transmises par l'intermédiaire de la plate-forme nationale des interceptions judiciaires qui organise la centralisation de leur exécution. […] »

d'infrastructures aptes à mettre en œuvre le TEJ, une difficulté supplémentaire apparaît en matière de budget, prohibant une dérive notable d'un budget initial. En effet, il existe un maillage des enquêteurs spécialisés sur le territoire[1507]. Ce sont donc une multitude d'infrastructures informatiques qui seraient concernées par l'éventuelle mise en œuvre du TEJ. Le risque d'une dérive budgétaire est alors beaucoup plus important qu'avec la PNIJ puisque ce n'est pas une seule plateforme technique qui est concernée, mais un nombre important. De plus, la même contrainte existe pour les frais de maintien en condition opérationnelle et la formation des agents et des militaires habilités.

903. Ainsi, outre le fait qu'il ne serait pas réaliste de concevoir une infrastructure technique augmentant de manière démesurée les coûts d'investissement et de fonctionnement actuels, le risque en cas de dérive du budget initial est exponentiel par rapport une évolution comme celle connue avec la PNIJ[1508]. La mise en œuvre du traitement d'exploitation judiciaire ne serait donc possible qu'au travers d'un *hardware* s'inscrivant dans une évolution mesurée des solutions actuellement utilisées par les enquêteurs spécialisés.

904. La solidité du socle de l'environnement technique existant. – Pour l'heure, hormis un manque chronique de disques durs pour procéder aux images des supports numériques saisis, l'environnement technique utilisé par les enquêteurs spécialisés leur permet de répondre aux missions qui leurs sont confiées.

905. La nécessité de rationaliser l'environnement technique existant. – Comme précédemment expliqué, les enquêteurs spécialisés que sont les N'Tech au sein de la Gendarmerie et les ESCI pour la Police, procèdent aux analyses de premier niveau[1509]. A ce titre, ils travaillent avec un environnement technique léger, qui pourrait même être qualifié « d'artisanal », à l'identique de ce qu'utilisent des experts civils[1510]. Cet existant devrait donc être rationalisé pour répondre aux exigences juridiques et permettre la mise en œuvre du TEJ.

Ministère de la Justice, *Projet de loi de programmation 2018-2022 et de réforme pour la justice – Rapport Annexe*, 23 avril 2018 : « […] l'obligation d'usage de la plateforme nationale des interceptions judiciaires (PNIJ), qui assure désormais plus de 90 % des prestations annexes et des interceptions judiciaires […]. »

[1507] V. *infra* n°946.

[1508] ALONSO Pierre et FANSTEN Emmanuel, *La PNIJ, gouffre à fric*, 14 mars 2016 : « Plus de 90 millions d'euros ont déjà été engloutis dans la Plateforme nationale des interceptions judiciaires. Une gabegie dont s'est saisie la Cour des comptes. »

[1509] V. *supra* n°338.

[1510] V. *supra* n°339.

906. La rationalisation de l'espace de stockage. – En premier lieu, le traitement d'exploitation judiciaire imposerait que les données soient strictement cloisonnées entre les procédures[1511]. Cela signifie que l'espace de stockage, c'est-à-dire l'endroit où seraient copiées l'ensemble des données issues des actes alimentant le TEJ, doit être conçu pour créer un volume[1512] dédié à une procédure. Or, actuellement, le matériel avec lequel travaille les enquêteurs spécialisés est constitué d'un ordinateur à l'intérieur duquel ils remanient régulièrement les disques durs dont ils ont besoin[1513]. Ce type de configuration ne répond pas aux exigences de cloisonnement. Le matériel mis à disposition des enquêteurs devrait, avec la mise en œuvre du TEJ, permettre la création d'un container numérique « étanche » affecté à un dossier. Toutes les données collectées ou générées au cours de l'enquête seraient appelées à y être enregistrées. Techniquement, la création d'un tel espace de stockage ne pose pas de difficulté, tout particulièrement pour la réalisation du cloisonnement entre des procédures distinctes.

907. En revanche, les données collectées pourraient rapidement représenter des quantités très importantes. De nos jours, un disque dur grand public de 2 To coute moins de 100 €. Ainsi, une « simple » saisie de matériels informatiques lors d'une perquisition au domicile d'un particulier qui télécharge beaucoup de films, peut nécessiter une grande capacité de stockage.

908. Cet espace, multiplié par le nombre de procédures en cours au sein d'une unité de police judiciaire, génèrerait une contrainte majeure en termes de capacité de stockage de l'infrastructure informatique. Qui plus est, la problématique se trouve accentuée par les longs délais des procédures, spécialement en matière criminelle.

909. Il faudrait donc rationaliser la gestion du stockage des données dans les configurations qui sont fournies aux enquêteurs spécialisés tout en restant réaliste. Un matériel de type NAS[1514] connecté par une liaison à très haut débit[1515] à la station procédant aux analyses, pourrait offrir un bon compromis entre une solution

---

[1511] V. *supra* n°819.

[1512] On parle de volume au sujet d'un espace de stockage qui n'a pas forcément d'existence physique. Il peut s'agir d'une subdivision d'un disque dur ou, au contraire, d'un regroupement de deux disques durs qui n'est vu que comme un seul espace de stockage par le système d'exploitation (l'objectif est dans ce second cas d'obtenir un volume de grande capacité).

[1513] V. *infra* n°909.

[1514] *Network Attached Storage*. : serveur de stockage en réseau. Un NAS est un espace de stockage externe à l'ordinateur qui exploite les données.

[1515] L'exploitation des informations numériques suppose de pouvoir analyser une grande quantité de données. Il existe différentes technologies pour connecter le NAS à l'ordinateur qui exploite les données. Dans le cas présent, une technologie offrant un débit important doit être privilégiée.

professionnelle[1516] et apportant de la souplesse avec l'espace disque. L'utilisation de disques durs SSD[1517] contribuerait également à améliorer les temps de traitement. En revanche, dans le souci de concevoir une solution réaliste d'un point de vue budgétaire, il est indispensable que ce soit la même configuration qui soit fournie à tous les services concernés, afin que les enquêteurs spécialisés de différentes unités puissent s'échanger des disques durs en fonction de besoins ponctuels plus importants.

910. La rationalisation d'un outil de sauvegarde. – En second lieu, dans l'objectif de rationaliser l'infrastructure physique mise à disposition des enquêteurs spécialisés, il serait indispensable de doter leur configuration d'un outil de sauvegarde sur des supports de grande capacité[1518]. Ces outils de sauvegarde permettraient de gérer la longueur d'une procédure en retirant les données de l'espace de stockage, tout en gardant la possibilité de pouvoir les réintroduire dans le système si un nouvel acte ou un nouvel élément nécessite de nouvelles analyses. En effet, comme précédemment expliqué, l'ensemble des données recueillies ou générées au cours d'une enquête pénale peuvent représenter un volume très important[1519]. Il ne serait donc pas concevable de conserver les données de toutes les procédures en cours enregistrées dans l'espace de stockage. L'outil de sauvegarde permet donc de les retirer provisoirement[1520], sans perdre l'état d'avancement dans lequel elles se trouvent.

911. Un deuxième intérêt pour l'outil de sauvegarde. – L'article R40-40 du Code de procédure pénale tel qu'il est proposé dans sa nouvelle forme[1521] prévoirait « qu'à la clôture de l'enquête, […] une copie informatique de l'ensemble des données et informations exploitées est placée sous scellés ou scellés numériques ».. Ce matériel de sauvegarde permettrait d'écrire ces données sur un support pouvant ainsi être mis sous scellés.

[1516] En tout état de cause moins artisanale que celle qui consiste à « *racker* » (anglicisme qui vient du mot « *rack* » qui désigne les logements au sein d'un ordinateur prévus pour recevoir des disques durs) des disques durs dans une tour : v. *supra* n°905.
[1517] Les disques durs de technologies SSD ne sont pas des disques durs mécaniques mais reposent sur des mémoires comme celles utilisées dans les clés USB. Les temps d'accès sont donc beaucoup plus rapides.
[1518] Par ex. des bandes magnétiques de type LTO.
[1519] V. *supra* n°907.
[1520] Par ex., au stade de l'information judiciaire, lorsque l'exécution d'une commission rogatoire est terminée et que les enquêteurs sont en attente d'une nouvelle demande du juge d'instruction.
[1521] V. annexe 3, projet de décret, article 9 venant modifier l'article R40-40.

912. Conclusion du sous-paragraphe I : la mise en œuvre de l'infrastructure physique. – La proposition de créer le traitement d'exploitation judiciaire comporte un premier volet relatif à la mise en œuvre technique : l'évolution de l'infrastructure actuelle dont disposent les enquêteurs spécialisés. Cette infrastructure constitue un socle solide sur lequel la mise en œuvre du TEJ pourrait s'appuyer efficacement. Néanmoins, deux évolutions seraient nécessaires. La première concernerait le stockage des données obtenues par l'ensemble des investigations numériques alimentant le TEJ. Outre une augmentation nécessaire de la capacité de stockage, des unités de stockage permettant de satisfaire aux exigences « d'étanchéité » des données d'une procédure par rapport à l'autre, serait indispensable. La seconde consisterait à équiper les enquêteurs spécialisés d'un outil de sauvegarde performant qui leur permettrait de gérer la longueur des procédures en ne conservant pas les données d'une enquête enregistrées en permanence au sein de l'espace de stockage. Cette unité de sauvegarde permettrait également de pouvoir placer sous scellés l'ensemble des données exploitées au sein du TEJ à la fin d'une procédure.

913. Un deuxième volet de la mise en œuvre technique doit être étudié. Il concerne l'évolution des logiciels utilisés pour exploiter les données au sein du TEJ.

II – La mise en œuvre des logiciels

914. La nécessité de choisir des logiciels adaptés aux contraintes légales du TEJ. – L'étude des logiciels permettant d'analyser l'ensemble des données obtenues au cours d'une enquête constitue un point essentiel de la mise en œuvre technique du traitement d'exploitation judiciaire. En effet, ces logiciels doivent respecter le cadre légal et réglementaire proposé[1522]. Or, jusqu'à présent, c'est le coût qui a guidé les services de l'Etat dans le choix des logiciels, puisque, comme précédemment expliqué, les enquêteurs spécialisés sont implantés en de nombreux points du territoire[1523]. Par voie de conséquence, le choix d'un logiciel se traduit par un nombre important de licences et donc un coût proportionnel. Bien évidemment, le budget découlant des conséquences de la création d'un traitement d'exploitation judiciaire serait une contrainte forte, afin de

[1522] V. *supra* n°824. Annexe 2 : Proposition de loi visant à améliorer l'efficacité et à renforcer les garanties des traitements de données en procédure pénale, Chapitre premier : Dispositions relatives aux traitements d'exploitation judiciaire.
V. *supra* n°825. Annexe 3 : Projet de décret relatif à la mise en œuvre des traitements à des fins d'exploitation et de rapprochement judiciaires.
[1523] V. *supra* n°902.

garantir que l'exploitation consolidée de l'ensemble des données collectées au sein d'une enquête reste crédible et puisse être généralisée pour toutes les procédures[1524]. Pour autant, la création d'un tel traitement imposerait de nouvelles contraintes telles que le cloisonnement par procédure ou la traçabilité de la provenance des données utilisées pour parvenir à une preuve[1525]. Dès lors, pour envisager la mise en œuvre du TEJ, le choix des logiciels *forensiques* devrait prioritairement être guidé par les fonctionnalités de ces derniers.

915. Le prolongement du *hardware* pour la séparation des procédures. – Les enquêteurs spécialisés travaillent sur un nombre important de dossiers en parallèle[1526]. Il serait interdit de procéder à du rapprochement entre des données issues de procédures différentes en application du TEJ[1527]. Comme précédemment expliqué[1528], l'infrastructure physique mise à disposition des agents ou militaires procédant à l'exploitation des informations numériques devrait permettre ce cloisonnement. Il en est de même avec les logiciels au sein desquels la distinction entre les différents dossiers doit pouvoir être facilement réalisée.

916. La nécessité d'une double traçabilité. – Le respect des droits de la défense et des libertés individuelles serait considérablement amélioré si une meilleure traçabilité était réalisée lors de l'exploitation des données personnelles recueillies au sein des différentes investigations numériques[1529] et si, surtout, les informations inhérentes à la traçabilité étaient versées au dossier de procédure. Or, deux types de traçabilité sont à distinguer.

917. En premier lieu, l'ensemble des accès aux logiciels permettant l'exploitation des données devrait faire l'objet d'un processus informatique reposant sur une authentification des enquêteurs spécialisés[1530], qui devraient avoir été préalablement

---

[1524] V. *supra* n°898.
[1525] V. *supra* n°892.
[1526] V. *supra* n°908.
[1527] Puisque le traitement d'exploitation judiciaire découle des logiciels de rapprochement judiciaire : v. *supra* n°819.
[1528] V. *supra* n°906.
[1529] Puisque toutes les investigations numériques ont pour effet de manipuler des données personnelles. V. *supra* n°808.
[1530] Sur la traçabilité informatique, v. DE GALZAIN Jean-Noël, *Nos PME doivent chasser en meute dans la cybersécurité*, L'Usine Nouvelle, 4 oct. 2013 : « Jean-Noël de Galzain, PDG et fondateur de la PME Wallix spécialisée dans la traçabilité informatique […]. »

habilités[1531]. Toutes les recherches et les manipulations effectuées sur les données devraient également être « historisées[1532] ». En second lieu, la provenance des informations exploitées au sein du traitement d'exploitation judiciaire devrait être tracée au sein de toutes les recherches effectuées. Ces informations devraient pouvoir être fournies au juge dans le cas où une nullité serait prononcée à l'encontre de l'une des investigations numériques dont les données ont alimenté le traitement[1533].

918. Une offre de logiciels limitée. – Les logiciels *forensiques* ne sont pas nombreux[1534]. Certains d'entre eux répondent nativement[1535] aux deux critères de traçabilité. La gestion des accès s'effectue de manière classique, avec différents profils permettant de différencier les droits au sens informatique du terme, notamment sur les dossiers (et donc les procédures) auxquels l'agent ou le militaire qui se connecte est autorisé à accéder. Le choix du logiciel par les autorités publiques doit donc prendre en compte ces nouveaux critères.

919. Un projet technique global. – La nécessité de fournir une solution apte à respecter le cloisonnement des dossiers les uns par rapport aux autres montre que les logiciels et le *hardware* doivent être étudiés conjointement. Pour gérer ce type de projet et concevoir une solution globale précise, il existe des services spécialisés au niveau de l'Etat. Il s'agit tout particulièrement du Service des Technologies et des Systèmes d'Information de la Sécurité Intérieure[1536], au sein du Ministère de l'intérieur. Ce service a l'expérience de coordonner de tels dossiers, en liaison étroite avec la Chancellerie et l'ANSSI[1537].

920. La nécessité d'une évolution plus importante à long terme. – L'objectif de la présente étude est de démontrer la faisabilité d'une analyse conjointe de toutes les données recueillies ou générées au sein d'une enquête pénale. Cette faisabilité doit donc reposer sur une solution technique réaliste d'un point de vue budgétaire, ce qui suppose

[1531] V. *supra* n°849.
[1532] Historiser : « néologisme informatique qualifiant l'action qui consiste à stocker des renseignements, des données, en vue de retrouver un historique. » Source : www.linternaute.fr
[1533] V. *supra* n°892.
[1534] Les deux plus connus sont *Encase* de l'éditeur Guidance Software et *Forensic Toolkit* d'Access Data.
[1535] C'est-à-dire sans avoir besoin d'avoir recours à du développement spécifique (adaptations personnalisées d'un logiciel).
[1536] Connu sous l'acronyme ST(SI)².
[1537] V. *supra* n°131.

de ne pas chambouler totalement les configurations informatiques actuellement utilisées par les enquêteurs spécialisés.

921. En revanche, un projet d'avenir pourrait consister à envisager de basculer les analyses de ces données dans une architecture industrielle. Un regroupement des moyens techniques en un (ou quelques) lieu(x) s'inscrirait dans le contexte de dématérialisation des infrastructures qui s'est installé depuis une décennie. Ainsi, les espaces de stockages évoqués pourraient être regroupés dans un *data center* centralisé. Celui-ci permettrait de mutualiser les espaces de stockages afin de répartir ceux-ci dynamiquement, puisque les besoins locaux sont tributaires des affaires en cours et ne sont donc pas constants.

922. Néanmoins, dans le contexte des analyses de données, ce raisonnement se heurte à deux difficultés qui nécessitent une étude technique d'envergure. La première est le débit réseau qui reste inégalitaire sur notre territoire, malgré les efforts conséquent de l'Etat en la matière. Or, les analyses de données nécessitent des transferts de données très importants[1538]. La deuxième difficulté est le changement complet de l'environnement informatique des enquêteurs ce qui, comme précédemment évoqué[1539], mérite d'être parfaitement maîtrisé afin de rester sur une exploitation réaliste, notamment pour prendre en compte le niveau de compétences requis.

923. La difficulté est la même pour les logiciels puisque, eu égard aux accès aux données très importants qui sont nécessaires, notamment pour l'indexation[1540], ceux-ci devraient, dans une telle configuration, être déportés au sein de l'infrastructure pour garantir le débit avec les données. Dès lors, c'est une architecture de type *cloud*[1541] qui se dessinerait et les postes de travail locaux sur lesquels travailleraient les enquêteurs, ne feraient que remonter les résultats de l'analyse. L'une des difficultés avec ce type d'architecture, qui justifie qu'il ne peut s'agir que d'une évolution à long terme, moyennant une étude approfondie, est de pouvoir concilier la simplicité de la mise en œuvre[1542] et la performance, avec le coût global à l'échelle du territoire national, qui pourrait rapidement devenir exorbitant notamment en raison du débit des accès réseaux qui doit être garanti à tous les sites hébergeant une équipe d'enquêteurs spécialisés.

[1538] Par ex. l'indexation, qui doit être exhaustive pour être efficace (seuls les fichiers systèmes sont identifiés et écartés par le logiciel *forensique*) et la reconstruction des données effacées peut prendre plus de 24H00 pour un disque dur de 2 To. Durant cette période, les accès disques sont permanents.

[1539] V. *supra* n°897.

[1540] Il s'agit d'une étape qui consiste à référencer toutes les chaînes de caractères présentes dans les données à analyser. C'est cette étape qui rend possible et efficace les recherches par mots clés : v. *supra* n°762.

[1541] V. *supra* n°221.

[1542] Une telle architecture induirait un bouleversement complet de la façon de travailler des enquêteurs spécialisés.

924. En revanche, tendre vers une telle architecture contribuerait à améliorer la traçabilité des accès aux données ainsi que le cloisonnement, car des telles applications en mode distribué pourraient fonctionner sur des instances différentiés[1543].

925. Conclusion du paragraphe §1 : la mise en œuvre technique du TEJ. – La proposition de créer le traitement d'exploitation judiciaire impose que la mise en œuvre technique de cette mesure permettant l'analyse, ensemble, de toutes les données obtenues au travers d'actes intrusifs[1544], soit réaliste et ne suppose pas des coûts exorbitants. La mise en œuvre technique se décompose en deux parties. En premier lieu, l'infrastructure technique[1545] pourrait s'appuyer sur les équipements actuels des enquêteurs spécialisés moyennant l'amélioration des outils de stockage et l'ajout d'une unité de sauvegarde performante. En second lieu, les logiciels appelés à être utilisés nécessiteraient, pour leur part, un investissement plus important. En effet, le cadre légal et réglementaire proposé leur impose de cloisonner les données procédure par procédure, et de permettre une traçabilité totale des investigations.

926. Les aspects techniques ne sont pas les seuls qui doivent être étudiés pour s'assurer que la mise en œuvre du TEJ soit réaliste, puisque les conséquences de la création d'un tel acte sur l'organisation des personnes intervenant dans les investigations numériques doivent également être mesurées.

§2. La mise en œuvre organisationnelle du TEJ

927. Une mise en œuvre organisationnelle[1546] crédible. – La proposition de créer le traitement d'exploitation judiciaire a pour objectif de permettre d'analyser, ensemble, toutes les données obtenues au sein d'une enquête pénale. Comme précédemment expliqué[1547], pour que ce projet de création soit crédible, outre un cadre légal et réglementaire réaliste, il est nécessaire que la mise en œuvre organisationnelle du TEJ ne nécessite pas un chamboulement total des services de police et de gendarmerie, notamment relatif au déploiement actuel des enquêteurs spécialisés[1548] sur le territoire.

[1543] C'est-à-dire qu'une instance du logiciel serait consacrée à une procédure.
[1544] V. *supra* n°235.
[1545] V. *supra* n°912.
[1546] Dictionnaire Larousse : « Qui concerne l'organisation d'un groupe, d'une entreprise, etc. »
[1547] V. *supra* n°897.
[1548] V. *supra* n°323.

928. La nécessaire adaptation de l'organisation de la mise en œuvre des investigations numériques intrusives. – Pour autant, l'étude de la mise en œuvre du TEJ doit dépasser celui-ci, pour s'inscrire dans une nécessaire adaptation organisationnelle plus globale de l'exécution des investigations numériques intrusives[1549]. En effet, il ressort de la présente étude que le rôle des experts judiciaires et des enquêteurs spécialisés, notamment en matière de fouille de données mises sous scellés manque de clarté[1550].

929. En conséquence, l'étude de la mise en œuvre du TEJ est réalisée au sein d'une étude de l'adaptation de l'organisation de l'exécution des investigations numériques intrusives. En premier lieu, le positionnement des experts judiciaires devrait être redéfini *(I)*. En second lieu, l'organisation des enquêteurs spécialisés nécessiterait certaines adaptations *(II)* pour permettre au TEJ d'améliorer l'exploitation des données obtenues au sein de l'enquête.

I – L'adaptation de l'intervention des experts judiciaires

930. L'inadaptation actuelle de l'intervention des experts judiciaires en « informatique[1551] » en enquête pénale. – Plusieurs difficultés liées à l'intervention des experts judiciaires au sein des investigations numériques ressortent des présents travaux. Ces difficultés, dues aux spécificités des investigations numériques, ont été mises en évidence à différentes étapes de la présente étude, comme au travers de la pluralité des régimes des investigations numériques, ou de la nécessité de créer un « savoir » au sein d'une enquête. Il est donc nécessaire de revenir sur l'ensemble des difficultés précédemment évoquées *(A)*, pour avoir la capacité de proposer une adaptation de l'intervention des experts judiciaires en informatique au sein d'une enquête pénale *(B)*.

A. Les difficultés liées à l'intervention des experts judiciaires

931. Des délais trop longs. – En premier lieu, c'est le délai de réalisation des expertises qui n'est pas compatible avec les contraintes des enquêtes, tout particulièrement policières[1552].

[1549] V. *supra* n°235.
[1550] V. *supra* n°422.
[1551] Il n'existe pas de catégorie « informatique » ou « numérique », explicitement désignée comme telle, au sein de la classification des listes d'experts judiciaires. V. *supra* n°302.
[1552] Entre deux et quatre mois : v. *supra* n°346.

932. L'imbrication des investigations numériques. – En deuxième lieu, ces délais sont incompatibles avec les besoins de rapidité imposés par la nécessaire imbrication des investigations numériques les unes avec les autres[1553]. En effet, les actes permettant de d'investiguer sur les données générées ou manipulées par un individu[1554] sont souvent liés les uns aux autres. Par exemple, la fouille d'un disque dur[1555] précédemment mis sous scellés lors d'une perquisition[1556], révèle aux enquêteurs la nécessité de procéder à une enquête sous pseudonyme sur un forum[1557], ou de réquisitionner un opérateur de téléphonie pour identifier le propriétaire d'un numéro de téléphone[1558]. Or, la volatilité des informations numériques[1559] impose aux enquêteurs de pouvoir enchaîner ces différentes investigations avec rapidité, au risque que des preuves soient perdues. L'intervention des experts judiciaires en informatique, lorsqu'ils sont commis pour une expertise ou réquisitionnés pour analyser des scellés numériques[1560], empêche cette imbrication des investigations numériques les unes par rapport aux autres, puisque les enquêteurs, seuls habilités à procéder à l'enquête sous pseudonyme ou à la réquisition d'un tiers dans l'exemple précédent, ne pourront procéder à ces actes que lorsque l'expert aura rendu son rapport à la fin de sa mission[1561]. Ainsi, une difficulté majeure est soulevée par l'intervention des experts, car celle-ci engendre une rupture dans la continuité et l'enchaînement des investigations numériques puisque les informations enregistrées dans un support ne prennent sens qu'en lien avec des données qui ne sont accessibles qu'au travers d'Internet [1562].

933. Le savoir de l'enquête. – En troisième lieu, les investigations numériques présentent la spécificité d'exploiter le savoir qui se crée au sein d'une enquête, plus que les autres investigations technologiques comme, par exemple, les analyses ADN. En effet, les analyses des données obtenues au travers d'une investigation numérique ne peuvent se faire efficacement qu'avec ce savoir[1563]. Ce dernier est indispensable pour les

[1553] V. *supra* n°788.
[1554] Ecoutes téléphoniques, réquisition d'un opérateur, captation de données, etc.
[1555] V. *supra* n°293.
[1556] V. *supra* n°244.
[1557] V. *supra* n°462.
[1558] V. *supra* n°372.
[1559] V. *supra* n° 223.
[1560] V. *supra* n°300.
[1561] V. *supra* n°791.
[1562] *Ibid.*
[1563] V. *supra* n°772.

recherches par mots clés, qui sont au cœur de l'exploitation des données[1564]. Lorsqu'un expert est saisi pour analyser un scellé contenant des données, il ne possède pas ce savoir que les officiers de police judiciaire en charge de l'enquête acquièrent petit à petit ce qui, par voie de conséquence, peut nuire à l'efficacité de l'analyse du scellé numérique confié à l'expert.

934. Le contournement du recours aux experts. – Les autorités publiques ont parfaitement pris conscience de ces différentes difficultés liées à l'intervention des experts judiciaires en informatique au sein des enquêtes pénales, puisque différentes dispositions ont été introduites dans le Code de procédure pénale pour permettre aux enquêteurs de conserver sous leur contrôle l'exploitation de tous les scellés numériques, sans avoir recours aux experts[1565].

935. Ces récentes dispositions[1566] sont des solutions palliatives pour contourner les difficultés, alors qu'il serait nécessaire de revoir l'intervention des experts judiciaires en informatique au sein des enquêtes pénales.

B. La proposition d'une intervention plus efficace

936. Le retour au rôle essentiel des experts. – Il serait erroné de conclure de l'ensemble des difficultés actuelles liées à l'intervention des experts judiciaires en informatique, que ces derniers ne devraient plus intervenir en procédure pénale. Pour appréhender la valeur ajoutée, bien réelle, que les experts peuvent apporter au sein d'une enquête, il est nécessaire de revenir aux sources de la commission d'expert. L'article 156 du Code de procédure pénale est sans ambiguïté : c'est « une question d'ordre technique » qui doit être posée aux experts. Si besoin est, l'article 158 accentue cette règle en précisant que « la mission des experts […] ne peut avoir pour objet que l'examen de questions d'ordre technique […] ». La spécificité des expertises consistant à analyser des scellés numériques a pour effet de transférer aux experts une partie de l'enquête[1567].

[1564] V. *supra* n°775.
[1565] V. *supra* n°348.
[1566] La possibilité de saisir un expert judiciaire pour procéder au clonage d'un support numérique dont la copie est analysée par les enquêteurs a été introduite par 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.
La création d'une liste d'enquêteurs spécialisés concurrente aux listes d'experts judiciaires a été réalisée par la loi n°2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice.
[1567] L'analyse des scellés numériques impose de procéder à une sorte de mini enquête : v. *supra* n°783.

937. Ainsi, pour repositionner justement et efficacement l'intervention des experts en informatique, un retour à la règle originelle de leur saisine devrait être opéré : au sein de l'enquête pénale, l'Homme de l'art, en informatique comme dans toutes les autres disciplines, est là pour apporter un éclairage à une question d'ordre technique, permettant la progression de la procédure. « L'enquête », au sens premier du terme[1568], doit être le domaine réservé des agents ou des militaires ayant une mission de police judiciaire et des magistrats du parquet et des juridictions d'instruction.

938. Un savoir technique complémentaire aux enquêteurs. – En procédure pénale, les experts devraient donc être saisis pour apporter aux autorités judiciaires leurs connaissances et leur savoir-faire dans des domaines ou des spécialités échappant, par nature, aux agents et militaires. C'est notamment le cas avec un domaine industriel ou professionnel particulier, un logiciel spécifique rencontré en analysant un support numérique, ou encore des techniques pointues de cryptage[1569]. C'est donc en étroite liaison avec les enquêteurs que l'intervention des experts en informatique peut se révéler la plus efficace et doit être concentrée. Ce travail collaboratif peut, par exemple, être préparatoire à une perquisition qui serait diligentée dans un environnement technique particulier et pour lequel les enquêteurs ont besoin de précisions pour préparer au mieux leur intervention sur site. La procédure permet cela sans aucune difficulté dès lors que la mission définie par le juge d'instruction pour l'expert, le lui demande. En ce sens, les articles 156 et 158 précités laissent une grande latitude[1570].

939. L'amélioration par le dépassement des listes d'experts judiciaires. – Le fait de recentrer le rôle confié aux experts sur des missions d'apport de compétences au service de l'enquête ne pose aucune difficulté en droit processuel puisque ceci s'inscrit dans les dispositions prévues par les textes. En revanche, un axe d'amélioration important en matière d'expertise informatique consisterait à faciliter la commission ou la réquisition de sachants en qualité d'expert, sans que ceux-ci soient inscrits sur l'une des listes

[1568] Dictionnaire Larousse : « Ensemble de recherches ordonnées par une autorité administrative ou judiciaire et destinées à faire la lumière sur quelque chose […] »
[1569] Sur les difficultés rencontrées par les autorités judiciaires face à des dispositifs de cryptage, v. *supra* n°422.
[1570] La jurisprudence veut que les mêmes règles soient transposées au stade de l'enquête avec la réquisition d'un expert, même si dans ce cas des difficultés subsistent : v. *supra* n°307.

d'experts judiciaires[1571]. En effet, le domaine de l'informatique et des systèmes d'information est particulièrement vaste. Derrière le mot « informatique » se trouvent un nombre difficile à définir de métiers, de compétences et de savoir-faire.

940. Aussi, il est impossible que les personnes inscrites sur une liste près une Cour d'appel possèdent les compétences couvrant l'ensemble du domaine, d'autant plus que les enquêteurs spécialisés ont aujourd'hui un bon socle de base et que, lorsqu'ils ont des besoins, ceux-ci sont nécessairement pointus et font appel à des spécificités très particulières, qui échappent aux enquêteurs.

941. L'obstacle par l'usage et non par la procédure. – L'article 160 du Code de procédure pénale prévoit, sans aucune ambiguïté, la possibilité d'avoir recours à un expert non inscrit[1572]. La contrainte imposée par le Code d'une prestation de serment préalable, ne soulève aucune difficulté car les juridictions d'instruction ou les enquêteurs appelés à réaliser ces saisines, disposent d'ores et déjà de documents préremplis pour cette prestation de serment, qui ne constitue donc pas un frein temporel à la fluidité de la mission. En revanche, l'usage induit une quasi obligation de commettre ou de requérir un expert dument inscrit. En effet, l'inscription sur l'une des listes d'experts s'accompagne de formations dispensées à l'expert par les compagnies d'experts judiciaires près une Cour d'appel et illustre donc une compétence de la personne inscrite au respect des procédures judiciaires. Pour autant, dans le cas de missions telles que celles qui viennent d'être décrites, où l'expert est sollicité par les enquêteurs ou le juge pour leur apporter un savoir spécifique, il se trouve encadré pour l'exécution de sa mission et ne risque pas de

---

[1571] Il existe une liste d'experts par Cour d'appel ainsi qu'une liste, dite liste nationale, qui est la liste des experts près la Cour de cassation, v. *supra* n°301.
En procédure pénale, à la différence des procédures civiles, la commission d'un expert qui n'est pas inscrit sur une liste doit être exceptionnelle et peut être une source de nullité : v. *supra* n°415.
C. pr. pén. art. 157 : « […] A titre exceptionnel, les juridictions peuvent, par décision motivée, choisir des experts ne figurant sur aucune de ces listes. »
SALATI Olivier, *Chapitre 121 – Liste nationale des experts judiciaires et listes dressées par chaque cour d'appel - Choix des experts sur ou hors des listes,* Dalloz Droit de l'expertise, 2016 : « Cette disposition [art. 157] d'ordre public étant édictée, d'après la chambre criminelle, dans l'intérêt d'une bonne administration de la justice, son inobservation par un juge d'instruction entache de nullité l'ordonnance de désignation. »
Crim. 8 juill. 2004 n°04-80.145 ; Bull. crim. n°180.

[1572] « Les experts ne figurant sur aucune des listes mentionnées à l'article 157 prêtent, chaque fois qu'ils sont commis, le serment prévu par la loi n°71-498 du 29 juin 1971 relative aux experts judiciaires devant le juge d'instruction ou le magistrat désigné par la juridiction. Le procès-verbal de prestation de serment est signé par le magistrat compétent, l'expert et le greffier. »
La sanction du défaut de prestation de serment est la nullité de l'expertise : Crim. 10 mai 2016 n°16-80.312.

nuire au bon déroulement des investigations qui restent sous le contrôle des autorités judiciaires.

942. Conclusion du sous-paragraphe I : l'adaptation de l'intervention des experts judiciaires. – L'exploitation des données obtenues par des actes intrusifs au cours des enquêtes pénales présente une spécificité par rapport à d'autres investigations technologiques. Pour que l'analyse des données soit efficace, ces dernières doivent être exploitées en lien les unes avec les autres. En effet, certaines informations numériques, par exemple présentes dans un disque dur saisi lors d'une perquisition, ne prennent sens que si elles sont exploitées conjointement avec des données recueillies au travers d'une captation des données. Dès lors, l'intervention des experts judiciaires en informatique, dont la mission consiste à analyser des scellés numériques, engendre une rupture dans l'imbrication indispensable entre les différentes investigations numériques. Seuls les enquêteurs peuvent enchaîner l'exploitation des données au travers des investigations numériques. Dans ce contexte, les experts judiciaires en informatique devraient être repositionnés sur des missions où ils auraient une véritable valeur ajoutée, telles que dans l'accompagnement des enquêteurs procédant à des investigations numériques, qui nécessitent une très haute compétence technique que les policiers ou les gendarmes ne possèdent pas forcément. Par exemple, la conception d'un outil permettant de procéder à une captation des données[1573], ou l'implantation de ce dispositif à distance[1574], pourrait être facilité si les enquêteurs bénéficiaient de l'appui technique d'experts dans les domaines correspondants. Toutefois, le déroulement de l'ensemble des opérations d'obtention des données et, surtout, de leur exploitation, devraient rester sous le contrôle des enquêteurs.

943. La proposition de création d'un traitement d'exploitation judiciaire est au cœur de cette nécessité de repenser le rôle des experts judiciaires en informatique, puisque le TEJ est l'outil qui aurait vocation à analyser les données obtenues et, qu'en aucun cas, il ne pourrait être mis en œuvre par les experts. Outre l'adaptation de l'intervention des experts, l'exploitation des données au sein du TEJ aurait également des effets sur l'organisation des enquêteurs spécialisés appelés à le mettre en œuvre.

[1573] V. *supra* n°580.
[1574] V. *supra* n°586.

II – L'adaptation de l'organisation des enquêteurs spécialisés

944. La nécessité d'une mise en œuvre organisationnelle mesurée. – Il est nécessaire d'étudier la mise en œuvre organisationnelle du nouvel acte d'enquête que serait le traitement d'exploitation judiciaire, afin de s'assurer que celle-ci serait réaliste. En effet, cette mise en œuvre ne doit pas nécessiter un chamboulement complet de l'organisation des services de Police et de Gendarmerie nationales. Au contraire, elle doit s'inscrire dans une évolution mesurée de ces derniers.

945. C'est pourquoi l'organisation actuelle doit être décrite *(A)* afin de pouvoir énoncer des propositions pour la mise en œuvre du TEJ *(B)*.

A. Le descriptif de l'organisation actuelle

946. L'organisation territoriale. – Il existe actuellement une différence importante sur l'organisation territoriale en vigueur entre la Police et la Gendarmerie[1575], pour ce qui est des enquêteurs spécialisés en numérique. La Gendarmerie a déployé au moins un N'Tech[1576] par département y compris dans les zones les plus rurales, et des pôles plus importants dans les villes où sont implantées des Sections de Recherche. Cette répartition est efficace puisqu'un officier de police judiciaire de la Gendarmerie peut solliciter un N'Tech qui se trouve à moins d'une heure, où qu'il se trouve sur le territoire national. Un tel délai répond aux besoins des enquêtes, tout particulièrement en cas de crime flagrant, où le besoin de préserver et de collecter les premiers éléments de preuve est déterminant. La police, pour sa part, a concentré ses efforts dans les grandes métropoles, au sein des SRPJ, et la présence d'ESCI[1577] dans les commissariats des villes de taille moyenne est aléatoire et dépend beaucoup de l'implication de certains agents dans le numérique.

947. La difficulté de la Police dans les villes moyennes. – De plus, une différence de fonctionnement entre la Gendarmerie et la Police accentue ce déficit de compétences dans les petits et moyens commissariats. Alors que la Gendarmerie fonctionne sur un mode de coopération territoriale fort[1578] avec une logique de mutualisation des ressources, la Police

---

[1575] ROUSSEL Gildas, *Police judiciaire – Organisation de la police judiciaire*, Dalloz Répertoire de droit pénal et de procédure pénale, 2019.
[1576] V. *supra* n°323.
[1577] *Ibid.*
[1578] Brigades Territoriales regroupées au sein d'une Compagnie, elles-mêmes regroupées dans un Groupement (qui correspond généralement à un département).
Ibid. ROUSSEL Gildas : « Depuis le décret n°2005-273 du 24 mars 2005, la gendarmerie nationale s'organise en vingt-deux régions divisées en groupements ou régiments (départements), eux-mêmes

est plutôt dans une structuration autonome pour chaque ville[1579]. Ainsi, l'enquêteur d'un commissariat d'une ville de taille moyenne est censé s'adresser au SRPJ de la métropole la plus proche pour répondre à un besoin particulier (tel que l'analyse de supports numériques lorsqu'il n'y a pas d'ESCI dans le commissariat concerné). Il y a là un problème, pour les agents de police judiciaire, qui ont donc des difficultés pour avoir accès aux enquêteurs spécialisés. Ce contexte doit être pris en compte lors de l'étude de la mise en œuvre du TEJ, même s'il s'inscrit dans un besoin organisationnel plus vaste.

948. L'organisation des ressources humaines. – Les analyses des supports numériques telles qu'elles sont actuellement réalisées donnent satisfaction. Cela signifie que les compétences des enquêteurs spécialisés constituent un socle solide sur lequel la proposition de mise en œuvre du TEJ peut s'appuyer. Néanmoins, une difficulté récurrente provient du manque de temps de ces agents ou militaires en raison des besoins qui augmentent fortement en la matière. Cette contrainte doit également être prise en compte pour le TEJ.

B. La proposition d'une mutualisation des ressources humaines

949. L'étude de la mise en œuvre du TEJ dans un contexte global. – L'organisation actuelle des enquêteurs spécialisés en numérique soulève deux difficultés majeures, qui sont, d'une part, la manque de ressources humaines pour faire face aux besoins grandissants en matière d'exploitation de données et, d'autre part, une inégalité territoriale pour les autorités judiciaires dans l'accès aux enquêteurs spécialisés. Ces deux difficultés, qui dépassent bien évidemment l'étude de la mise en œuvre du traitement d'exploitation judiciaire, doivent néanmoins être prises en compte. Ainsi, il ne serait pas réaliste de proposer une augmentation démesurée des ressources humaines pour rendre possible la mise en œuvre du TEJ. La proposition qui évoquerait un déploiement

---

comprenant des compagnies ou escadrons (arrondissements), qui comprennent des sections, pelotons ou brigades organisées ou non en communautés de brigades […]. »
C. défense art. R3225-7.

[1579] Le fait qu'il existe un DDSP (Directeur Départemental de la Sécurité Publique dans les départements ruraux et un Préfet de Police dans les grandes conurbations) n'a que peu d'effet sur la mutualisation des ressources en enquêteurs spécialisés.
C. sec. int. art. R431-8 : « […] Le directeur départemental de la sécurité publique, sans préjudice des compétences particulières des autres responsables des services de la police nationale dans le domaine qui est le leur, et le commandant de groupement de gendarmerie départementale sont, chacun dans son domaine de compétence, les conseillers du préfet en matière de sécurité et de paix publiques. »

d'enquêteurs spécialisés dans tous les commissariats de France, y compris les plus petits[1580], resterait purement théorique.

950. La nécessaire collaboration entre Police et Gendarmerie pour l'exploitation des données. – Pour être réaliste et mesurée, la nécessaire augmentation des agents et des militaires aptes à analyser des données passe par une collaboration opérationnelle forte entre la Gendarmerie et la Police nationales. L'objectif d'une intégration plus forte entre les forces de Police et de Gendarmerie n'est pas nouveau et s'inscrit dans une mutualisation des forces de l'ordre. Une loi de 2009 allait dans ce sens en posant un principe de rattachement de la Gendarmerie nationale au Ministère de l'intérieur[1581]. Mais un retour en arrière a eu lieu en 2012 en la rattachant à nouveau de manière principale au Ministère de la défense[1582]. En aucun cas, les présents travaux n'ont vocation à constituer une étude du rapprochement, voire de la fusion entre les deux forces de police françaises, qui constitue un sujet qui perdure depuis des années. Il ne s'agit ici d'évoquer cette collaboration, qu'au travers de l'exploitation des données obtenues au sein d'une enquête pénale.

951. La nécessaire création de pôles d'enquêteurs spécialisés en numérique. – Comme précédemment expliqué[1583], l'introduction d'un TEJ pour exploiter les données obtenues au sein de l'enquête ne rencontrerait aucune difficulté organisationnelle dans les grandes agglomérations, puisqu'il existe déjà une concentration des enquêteurs spécialisés en numérique au sein des commissariats ou des gendarmeries dans ces zones géographiques. En revanche, ce point devient sensible dans les départements au sein desquels aucune métropole de taille importante n'est présente. Or, le réseau en enquêteurs spécialisés est mieux réparti au sein de la Gendarmerie. Dès lors, il semble pertinent de s'appuyer sur celui-ci, moyennant une augmentation raisonnable des ressources humaines qui serait de toute façon inéluctable, plutôt que de s'engager dans une voie qui consisterait à doter les commissariats de petites tailles, d'agents qui se retrouveraient isolés. Ainsi, la

[1580] Il subsiste des hôtels de police dans des bourgades rurales de moins de 10 000 habitants malgré la suppression, ces dernières années, de certains commissariats de petite taille pour les basculer dans les zones Gendarmeries. Ex. : Graulhet dans le Tarn. Une autre stratégie de l'Etat consiste à fusionner des commissariats : ORTIZ Sébastien, *Les commissariats rapprochés 2 par 2*, L'Eclaireur du Gâtinais,1 janv. 2020.
[1581] Loi n°2009-971 du 3 août 2009 relative à la gendarmerie nationale.
[1582] Ordonnance n°2012-351 du 12 mars 2012 relative à la partie législative du code de la sécurité intérieure : v. la rédaction actuelle de l'art. L3225-1 du Code de la défense telle qu'elle résulte de ce texte.
[1583] V. *supra* n°946.

création de pôles composés de plusieurs individus serait nécessairement plus efficace[1584] que des agents seuls.

952. En s'appuyant sur le maillage existant de la Gendarmerie, ces pôles seraient à moins d'une heure de tous les officiers de police judiciaire[1585], ce qui répond à l'exigence d'utiliser le « savoir de l'enquête » pour procéder à l'exploitation des données[1586]. En effet, il est indispensable pour l'efficacité des analyses de données, notamment pour les recherches par mots clés, que les analyses soient réalisées par un enquêteur qui est au cœur de l'enquête ou, à tout le moins, qui travaille en étroite collaboration avec les officiers de police judiciaire en charge du dossier. Pour que cette collaboration soit possible et efficace, la proximité géographique est une source évidente d'efficacité.

953. La cohérence des pôles d'enquêteurs spécialisés avec les dispositions proposées. – La création de tels pôles pourrait avoir pour effet que ce soit un service de la Gendarmerie qui procède à l'exploitation des données au sein d'une enquête confiée à un service de Police. Cette situation est parfaitement compatible avec le cadre légal et règlementaire proposé pour le traitement d'exploitation judiciaire. En effet, le projet de décret relatif à la mise en œuvre des traitements à des fins d'exploitation et de rapprochement judiciaires, propose d'introduire une nouvelle version de l'article R40-40 dans le Code de procédure pénale qui disposerait que « la mise en œuvre des traitements […] est autorisée, pour chaque procédure qu'il contrôle, par le magistrat saisi de l'enquête ou chargé de l'instruction[1587] ».

954. Or, il n'existe aucun lien formel entre une éventuelle commission rogatoire délivrée par un juge d'instruction ou une enquête, qui serait confiée à un service de police judiciaire et l'autorisation de mise en œuvre d'un TEJ telle que proposée. Cette répartition des tâches s'inscrit parfaitement dans la dissociation entre l'obtention des données au travers des investigations numériques et leur exploitation au sein du TEJ[1588]. Les informations numériques sont recueillies ou générées par les officiers de police judiciaire en charge de l'enquête. Avec la mise en œuvre du TEJ, ils coordonneraient les analyses des données qui seraient effectuées par le pôle regroupant les enquêteurs spécialisés. Cette coordination serait possible grâce à la proximité géographique.

[1584] Notamment pour gérer les absences et les permanences des enquêteurs spécialisés.
[1585] V. *supra* n°946.
[1586] V. *supra* n°772.
[1587] Annexe 3, projet de décret, art. 9.
[1588] V. *supra* n°832.

955. Conclusion du titre 1 : la nécessité de regrouper les données obtenues par les actes intrusifs. – Actuellement, l'analyse des données recueillies ou générées au travers des investigations numériques est réalisée au sein de l'acte ayant permis leur obtention. Cette liaison entre l'acte et les données obtenues a pour effet de cloisonner les données acte par acte. Or, ce cloisonnement nuit potentiellement à l'efficacité de l'exploitation des données. En effet, cette dernière pourrait être beaucoup plus performante, si toutes les données obtenues au sein d'une enquête, pouvaient être analysées ensemble.

956. Une telle possibilité serait possible, sans chamboulement majeur de la procédure pénale, en modifiant les dispositions actuelles des logiciels de rapprochement judiciaire. En effet, ces derniers permettent d'ores et déjà de regrouper des informations issues de différentes sources. De plus, une décision du Conseil constitutionnel a restreint leur champ d'application aux informations d'une seule et même procédure. La présente étude énonce donc une proposition pour créer un « Traitement d'Exploitation Judiciaire » (ci-après « TEJ ») à partir d'une évolution des logiciels de rapprochement judiciaire, qui aurait pour finalité d'exploiter, conjointement, l'ensemble des données obtenues au sein d'une enquête pénale.

957. Outre la possibilité de créer un cadre légal et règlementaire qui permettrait de regrouper les données pour les exploiter, il est nécessaire d'étudier la mise en œuvre du TEJ. En effet, celle-ci doit être réaliste. En aucun cas, une nouvelle investigation numérique qui nécessiterait des moyens technologiques ou humaines exorbitants ne serait crédible, ou se retrouverait réservée à des dossiers d'une particulière importance.

958. En premier lieu, la mise en œuvre technique du TEJ nécessiterait une évolution mesurée des moyens techniques actuellement utilisés par les enquêteurs spécialisés. Cette évolution consisterait à améliorer l'équipement actuel afin qu'il puisse parfaitement répondre aux exigences légales et règlementaires proposées. Il s'agit notamment de pouvoir placer sous scellés, au terme d'une procédure, les données exploitées, et de pouvoir fournir au juge l'historique et la traçabilité de toutes les analyses effectuées.

959. En second lieu, la proposition de créer le TEJ doit également reposer sur une mise en œuvre organisationnelle crédible. Celle-ci pourrait être l'occasion de redéfinir l'intervention des experts judiciaires en informatique, en concentrant leur rôle sur un accompagnement des enquêteurs visant à leur fournir de hautes compétences, lorsque les besoins d'une enquête conduit ces derniers à intervenir dans un domaine ou sur des données qui dépassent leurs connaissances. En effet, il est essentiel que ce soit les enquêteurs qui procèdent à l'intégralité de l'exploitation des données obtenues lors des

investigations numériques, afin que ces analyses puissent se faire en étroite collaboration avec les officiers de police judiciaire qui conduisent l'enquête. Dans les départements les moins peuplés, la mise en œuvre du TEJ nécessiterait la création de pôles mutualisant les enquêteurs spécialisés de la Gendarmerie et de la Police nationales.

960. La proposition de créer un traitement d'exploitation judiciaire a pour objectif d'autoriser le regroupement des données obtenues au travers des investigations numériques intrusives. Elle n'est qu'une étape de l'amélioration de la prise en compte des données utiles aux enquêtes, puisque la consolidation des informations numériques contenues dans les multiples traitements judiciaires accessibles aux enquêteurs en constituerait une deuxième étape.

TITRE II. LA NECESSITE DE REGROUPER LES DONNEES DES TRAITEMENTS JUDICIAIRES

961. Le nécessaire dépassement des actes mettant en œuvre les investigations numériques. – Les investigations numériques en procédure pénale sont des actes d'enquête qui permettent l'obtention de données[1589]. L'extraction d'informations numériques depuis des traitements judiciaires[1590] constitue l'une des deux catégories d'investigations numériques[1591]. Les dispositions relatives aux traitements judiciaires sont éparpillées, non seulement au sein du Code de procédure pénale[1592], mais également dans une multitude de textes non codifiés[1593]. Cet éparpillement est inextricablement

[1589] V. *supra* n°191.
[1590] L'appellation « traitement judiciaire » désigne, dans les présentes, tout traitement de données à caractère personnel directement accessible aux autorités judiciaires au stade de l'enquête : v. *supra* n°609.
[1591] V. *supra* n°213.
[1592] V. par ex, C. pr. pén. Livre I[er], Titre IV : « Dispositions communes » pour les fichiers d'antécédents, les fichiers d'analyse sérielle, le fichier des personnes recherchées, la PNIJ, etc.
C. pr. pén. Livre IV, Titre XV : « De la poursuite, de l'instruction et du jugement des actes de terrorisme » pour le fichier judiciaire national automatisé des auteurs d'infractions terroristes.
C. pr. pén. Livre IV, Titre XIX : « De la procédure applicable aux infractions de nature sexuelle et de la protection des mineurs victimes » pour le fichier judiciaire national automatisé des auteurs d'infractions sexuelles ou violentes.
[1593] V. par ex. le décret n°87-249 du 8 avril 1987 relatif au fichier automatisé des empreintes digitales géré par le ministère de l'intérieur modifié par le décret n° 2015-1580 du 2 décembre 2015.
L'arrêté du 18 mai 2009 portant création d'un traitement automatisé de contrôle des données signalétiques des véhicules.
L'arrêté du 17 mars 2014 portant autorisation à titre expérimental d'un traitement automatisé de données à caractère personnel dénommé « Fichier des objets et des véhicules signalés » (FOVeS).

associé à une pluralité des régimes pour la consultation, l'alimentation et le contrôle des traitements judiciaires[1594].

962. Cet éparpillement et cette pluralité des régimes ne sont pas propres aux investigations numériques dans leur ensemble[1595]. Or, la présente étude n'a pas vocation à étudier une réforme de la procédure pénale dans son ensemble[1596], mais de proposer des améliorations des investigations numériques. Ces améliorations sont possibles en dépassant les actes de procédure que sont les investigations numériques, et en raisonnant sur la donnée, qui constitue leur spécificité principale commune.

963. Le constat du cloisonnement des données. – Une idée préconçue veut que la séparation physique des traitements judiciaires soit protectrice des libertés individuelles[1597] et protègerait mieux en cas d'acte de malveillance. Cette idée provient d'une erreur qui consiste à assimiler l'éparpillement des traitements[1598] et la séparation physique des données. En effet, les données sont le support numérique des informations[1599]. Il peut donc sembler évident, au premier abord, qu'en éparpillant les traitements au sein d'entités différentes, les données s'en trouvent séparées. Par voie de conséquence, les informations personnelles collectées le seraient alors nécessairement. Or, ce raisonnement ne tient pas compte de l'ensemble du contexte de la dématérialisation des informations.

964. Les conséquences négatives. – Au contraire, l'éparpillement des traitements induit évidemment un éparpillement des données. Or, d'une part, celui-ci n'implique pas forcément le cloisonnement des informations numériques. D'autre part, tel qu'il est actuellement réalisé, il nuit à la fois à la performance de l'exploitation des données en enquête, et au respect des libertés individuelles.

965. L'enjeu du regroupement des données des traitements judiciaires. – L'un des enjeux de la présente étude consiste à proposer un regroupement cohérent des données

---

[1594] V. *supra* n°605.
Sur le cadre législatif et règlementaire « foisonnant », v. PARIS Didier et MOREL-A-L'HUISSIER Pierre, *Rapport d'information sur les fichiers mis à la disposition des forces de sécurité*, déposé et enregistré à l'Assemblée nationale le 17 oct. 2018, p.21.
[1595] V. *supra* n°732.
[1596] Sur la réforme de la procédure pénale, v. *supra* n°732.
[1597] V. *infra* n°969.
[1598] L'éparpillement des traitements provient d'une pluralité de responsables de traitements (Gendarmerie, Police nationale, Ministère de l'intérieur, de la justice) , et du fait que les bases de données sont gérées et administrées au sens informatique du terme, par des entités différentes (Direction de la Gendarmerie, Direction de la Police judiciaire, service du Casier judiciaire, etc).
[1599] V. *supra* n°6.

enregistrées dans certains traitements judiciaires**.** Il serait irréaliste d'envisager la création d'une base de données unique rassemblant des traitements aux finalités et aux conditions de mise en œuvre très différentes, au seul motif qu'ils sont accessibles lors d'une procédure pénale.

966. Pour autant, il est nécessaire de rompre avec la vision erronée selon laquelle la multiplication de fichiers de police disséminés auprès de structures différentes, et donc composés de données physiquement éparpillées, est un facteur de protection des libertés individuelles *(Chapitre 1)*, pour pouvoir étudier la cohérence qu'apporterait la consolidation de certaines de ces données *(Chapitre 2)*.

Chapitre 1. La protection illusoire des personnes fichées par l'éparpillement des données

967. L'ambivalence de la notion de « personne fichée ». – Le mot « fichage » comporte une double connotation. Il se réfère à la fois à la notion juridique de traitements de données à caractère personnel et à la notion informatique de base de données. Historiquement, le mot « fichage » fait référence aux fiches cartonnées qui existaient autrefois, aussi bien dans les gendarmeries[1600] qu'au sein de la Police[1601]. Cette notion de « fiche » résiste dans le vocabulaire courant malgré la dématérialisation, puisque les médias parlent fréquemment d'individus « fichés S » pour des personnes faisant l'objet d'un suivi administratif pour radicalisme religieux[1602]. La doctrine n'hésite également pas à employer ce mot, y compris récemment[1603].

968. Ainsi, dans la présente étude, les expressions « fichiers[1604] », « traitements » et « base de données » sont employées comme des synonymes et regroupées sous la notion de « traitement judiciaire[1605] ». Comme précédemment expliqué, les traitements judiciaires sont tous les traitements de données pour lesquels un accès est directement prévu pour les autorités judiciaires au stade de l'enquête pénale[1606]. Ces traitements judiciaires sont souvent appelés « fichiers de police, » bien que les fichiers mis en œuvre par les forces de police ne représentent qu'une partie des traitements judiciaires puisque certains d'entre eux sont créés et gérés par des autorités purement administratives[1607].

[1600] Avec le fichier alphabétique du renseignement (FAR) qui était composé de fiches manuscrites présentes dans chaque unité opérationnelle de gendarmerie.
[1601] Avec le système de micro-fiches dénommé MIDOS.
[1602] « Fiché S » se réfère à l'inscription dans le fichier de traitement des signalements pour la prévention de la radicalisation à caractère terroriste (FSPRT).
Pour les traitements de données liés à la dangerosité des personnes, v. *infra* n°666.
[1603] V. par ex. :
MARTINELLE Mathieu, *L'utilisation des caractéristiques génétiques dans les procédures judiciaires*, Dalloz AJ pénal 2018 p.69.
VIBRAC Geoffrey, *Les fichiers à l'épreuve de nouveaux droits effectifs pour les personnes ?* Dalloz AJ pénal 2018 p.564.
[1604] Sur l'assimilation du mot « fichier » avec la notion de « traitement de données à caractère personnel, v. MAXWELL Winston et ZOLYNSKI Célia, *Protection des données personnelles*, Recueil Dalloz, 2019, p.1673 : « Pour cela, l'arrêt [CJUE 10 juill. 2018, aff. C-25/17] retient une interprétation extensive de la définition du fichier en affirmant que son caractère « structuré selon des critères déterminés » vise uniquement à permettre que « les données relatives à une personne puissent être retrouvées aisément » (par ex. par un classement par ordre alphabétique, une répartition géographique ou un simple aide-mémoire). »
[1605] V. *supra* n°609.
[1606] V. *supra* n°614.
[1607] V. *supra* n°696.

969. La crainte d'un fichage massif et généralisé. – Le fichage des individus, dont le seul mot comporte une connotation fortement péjorative pour le grand public, est un serpent de mer qui réactive régulièrement des débats dans la presse[1608], tant il subsiste une véritable crainte de notre société pour la surveillance massive des individus. A l'origine de cette situation, se trouve le mythe toujours bien présent dans les esprits de « *Big Brother*[1609] », qui révèle une inquiétude générale pour le fichage complet des individus. D'ailleurs, en 2008, les nombreuses réactions face à la création du fichier *Edvige* avaient contraint l'Etat à rebrousser chemin[1610].

970. La conséquence de la crainte du fichage massif et généralisé. – Face à cette crainte, l'Etat a fait le choix d'éparpiller les traitements judiciaires en confiant leur gestion à des entités différentes. Cet éparpillement a pour effet de disséminer physiquement les données.

971. L'illusoire protection de la séparation physique des données. – Or, l'éparpillement des données a majoritairement des conséquences négatives qui nuisent plus aux droits des personnes fichées que ce qu'elles les protègent[1611]. En premier lieu, la dissémination des informations numériques dans une multitude de fichiers différents est incohérente avec le respect et l'application des règles inhérentes à la protection des données personnelles *(Section 1)*. En second lieu, cet éparpillement compromet, pour des raisons techniques, la fiabilité et la qualité des données, ce qui a nécessairement pour conséquence de nuire aux droits des personnes fichées *(Section 2)*.

[1608] Comme à l'occasion de la tentative de création du fichier Edvige. V. Le Monde, 8 septembre 2008, p. 10, *Fichier Edvige : les points inquiétants pour les libertés.* Ou encore Libération, 4 septembre 2008, n°8501, *La vigilance autour d'Edvige :* « Le prénom est sympathique. Pourtant, il suscite crainte et défiance. »

[1609] Personnage imaginaire créé dans le roman « 1984 » de Georges ORWELL.

[1610] LAVRIC Sabrina, *Fichier EDVIGE : recours devant le Conseil d'Etat*, Recueil Dalloz 2008 p.2222.

[1611] Sur les droits des personnes fichées, v. GAUTRON Virginie, *Fichiers de police – Réglementation internationale*, Dalloz Répertoire de droit pénal et de procédure pénale, mars 2019, Section 1re - Instruments de protection adoptés par les États membres du Conseil de l'Europe : « 82. Les dispositions conventionnelles applicables. - Si plusieurs dispositions de la Convention [européenne de sauvegarde des droits de l'homme et des libertés fondamentales] sont applicables en matière de collecte, de stockage ou d'utilisation de données contenues dans des fichiers de police, les requêtes soumises à la Cour européenne des droits de l'homme évoquent principalement des violations de l'article 8 de la Convention, qui garantit le droit à la vie privée. »

Section 1. L'incohérence entre l'éparpillement et la protection des données personnelles

972. Une séparation logique et facile à mettre en œuvre avec peu de traitements. – Lorsque l'Etat a commencé à dématérialiser[1612] les informations personnelles qu'il devait collecter pour mener à bien ses différentes missions, le principe de séparation physique des données répondait parfaitement à la protection de notre société puisqu'un fichage général était ainsi évité. Ces fichiers avaient alors une finalité claire au sens des règles de la protection des données personnelles[1613], qui correspondait aux informations qui y étaient enregistrées.

973. L'inefficacité de la séparation physique des données face à la multiplication des traitements. – Cette situation initiale avec des traitements précis et ciblés est désormais totalement dépassée en raison de l'augmentation exponentielle des besoins de l'Etat en matière de collecte de données[1614]. Comme précédemment expliqué, en procédure pénale, il est aujourd'hui impossible de dresser une liste exhaustive des fichiers de police[1615]. Face à une telle multiplication des traitements judiciaires, il devient impossible de respecter, ou de faire respecter, certaines règles de la protection des données personnelles.

974. L'incompatibilité entre l'idée préconçue d'une protection des personnes par l'éparpillement des traitements judiciaires et les règles s'appliquant aux données personnelles se concrétise sous deux formes. En premier lieu, le besoin exponentiel de l'Etat en collecte de données pour répondre aux besoins des enquêtes pénales n'est plus compatible avec des traitements judiciaires aux finalités fortement spécialisées *(§1)*. En second lieu, la multiplication des traitements judiciaires éparpillés au sein d'entités différentes rend inapplicable les règles de la protection des données personnelles *(§2)*.

[1612] V. *supra* n°15.

[1613] Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, art. 4 : « Les données à caractère personnel doivent être […] 2° Collectées pour des finalités déterminées, explicites et légitimes, […] ».
Idem. RGPD (*op. cit.* p.12) art. 5.

[1614] GAUTRON Virginie, *Fichiers de police* – généralités, Dalloz Répertoire de droit pénal et de procédure pénale, mars 2019, : « Une amplification considérable du fichage. - La rationalisation des pratiques policières, voire la constitution d'une véritable « science des fichiers », a engendré une extension considérable du nombre de fiches conservées […]. »

[1615] V. *supra* n°615.

§1. L'incohérence avec une spécialisation excessive des traitements judiciaires

975. Une finalité unique par traitement non respectée. – La volonté de l'Etat d'éparpiller les traitements judiciaires est associée à une très forte spécialisation de ces derniers. Or, la spécialisation se traduit, en application de la loi informatique et libertés, par une finalité précise et unique[1616], et une collecte d'informations strictement nécessaires pour l'accomplissement de la finalité énoncée.

Le besoin de l'Etat en collecte d'informations pour répondre aux besoins de l'efficacité des enquêtes pénales est tel, que ce principe d'une finalité unique et lisible ne peut plus être respecté *(I)*. De plus, lorsqu'une finalité est énoncée, la description des données autorisées à être collectées ouvre un périmètre d'informations dépassant nettement cette finalité (*II)*.

I – L'incohérence avec la finalité

976. Le constat du non respect de la finalité unique des traitements. – La multiplication des besoins des autorités judiciaires en matière de collecte d'informations numériques[1617] met à mal la volonté de créer des fichiers spécialisés par finalité.

977. Le regroupement de finalités différentes. – Le fichier judiciaire national automatisé des auteurs d'infractions sexuelles ou violentes ne respecte pas ce principe d'une finalité unique. Comme précédemment évoqué[1618] le regroupement des auteurs d'infractions sexuelles et d'infractions violentes n'est pas cohérent car on n'est pas en présence des mêmes typologies criminelles, et ce rapprochement de finalités différentes dans un même traitement porte atteinte à sa lisibilité. Le fait de créer une base de données des individus ayant été condamnés pour des infractions sexuelles[1619] ainsi que pour toute infraction à caractère sexuel en relation avec des mineurs[1620] paraît logique en raison du caractère sériel reconnu de ces infractions. Le fait d'y avoir ajouté les « crimes de meurtre ou d'assassinat […] commis sur un mineur, précédés ou accompagnés d'un viol[1621] » procède du même raisonnement. En revanche, l'association avec des infractions violentes, mais sans aucun lien avec des délits ou des crimes sexuels, telles que les crimes de tortures ou d'actes de barbarie, ou la diffusion à l'attention de mineurs d'images

[1616] *Ibid.* Loi informatique et libertés art. 4.
[1617] V. *supra* n°973.
[1618] V. *supra* n°670.
[1619] V. C. pr. pén. art. 706-47 3° et 4°.
[1620] V. C. pr. pén. art. 706-47 6° au 13°.
[1621] V. C. pr. pén. art. 706-47 1°.

violentes[1622] est une entorse au principe de spécialisation des traitements de données judiciaires. Il y a là une sorte de regroupement de données judiciaires aux finalités différentes. D'ailleurs, certains auteurs voient dans ce fichier, « un véritable contrôle post-carcéral » qui dépasse nettement les infractions à caractère sexuel[1623].

978. Le constat de l'absence de clarté dans la dénomination des traitements. – La spécialisation des traitements judiciaires impose une autre contrainte, lors de la création d'un traitement de donnée à caractère personnel à vocation judiciaire : il est nécessaire de lui donner un nom clair et parlant pour l'ensemble des citoyens, permettant ainsi de connaître sans ambiguïté son utilité[1624].

979. Des fichiers de police au nom trompeur. – La plus forte incohérence dans la dénomination d'un traitement judiciaire est le Traitement d'Antécédents Judiciaires (TAJ)[1625], qui a vocation à recevoir les informations nominatives des personnes mises en cause mais également des victimes[1626] et des témoins. Il est profondément choquant qu'une victime soit fichée dans une base de données laissant supposer qu'elle a commis des faits judiciairement répréhensibles en raison du nom du traitement dans lequel elle fait l'objet d'un enregistrement[1627]. Après les péripéties ayant conduit à la création du TAJ[1628], le législateur aurait dû trouver un nom dont la connotation ne porte pas préjudice aux victimes, en les assimilant à des personnes ayant « des antécédents judiciaires ».

980. Conclusion du sous-paragraphe I : l'incohérence avec la finalité. – L'éparpillement des traitements judiciaires n'est plus compatible avec le besoin croissant en besoin de collecte d'informations personnelles par les autorités judiciaires pour assurer l'efficacité de l'enquête pénale. Tout d'abord, cette incompatibilité se manifeste au travers de l'incohérence entre les noms de certains traitements judiciaires et leur finalité,

---

[1622] Ex. : des images de torture, de propagande pour des jeux d'automutilation qui ont tendance à séduire les adolescents, etc.
[1623] MARGAINE Clément, *La loi du 15 août 2014 et le milieu ouvert : vers un accroissement du contrôle des personnes condamnées*, Dalloz AJ pénal 2014 p. 453.
[1624] GAUTRON Virginie, *Fichiers de police – Réglementation française,* Dalloz, Répertoire de droit pénal et de procédure pénale, Avril 2015.
[1625] V. *supra* n°642.
[1626] C. pr. pén. art. R40-26.
[1627] Sur la perception du « soupçon » que fait peser sur une personne le fait qu'elle soit fichée dans un fichier : v. MAROT Pierre-Yves, *Fonctions et mutations des fichiers de police*, Dalloz, AJ pénal 2007, p. 61 : « […] à partir du soupçon qu'il [le traitement judiciaire] fait peser d'emblée sur les individus fichés […]. »
[1628] V. *supra* n°644.

voire même avec un regroupement de plusieurs finalités, ce qui va à l'encontre de la volonté affichée.

981. Ensuite, une autre incompatibilité apparaît avec le périmètre des données qui dépasse la finalité annoncée.

II – L'incohérence entre la finalité et le périmètre des données

982. Un périmètre des données illégitimement étendu. – Certains traitements judiciaires comportent une incohérence entre la finalité annoncée, ou qui se dégage de leur dénomination, et la diversité des informations qui sont autorisées à y être enregistrées.

983. Comme précédemment expliqué[1629], le fichier des personnes recherchées est la première illustration de cette mise à mal de la spécialisation des traitements de données qui est censée découler de leur isolement. L'étude de ce traitement montre que sont notamment enregistrées dans la base de données, des personnes ayant fait l'objet d'une interdiction administrative de stade ou frappées d'une interdiction d'exercer certaines activités, ou encore qui sont sous le coup d'un retrait de permis de conduire[1630]. Ces différentes situations sont très éloignées de la notion de personnes recherchées, dont la signification est précisément d'être recherchées par la justice[1631].

984. Il existe également des traitements pour lesquels leur spécialisation n'est pas du tout évidente et qui tendent vers des bases de données au périmètre beaucoup plus vaste que ne le voudrait le principe de spécialisation. Certains fichiers, comme ceux de la police administrative, ont des intitulés généraux, vagues. De plus, la définition des données qui y sont enregistrées est floue, ouvrant ainsi un champ de collecte dont on ne cerne pas explicitement le contour. C'est le cas du PASP[1632] au sujet duquel la CNIL, dans sa délibération du 11 juin 2009, avait demandé que « la nature exacte des données susceptibles d'être enregistrées sous cette catégorie devrait être mieux définie[1633] ». La

---

[1629] V. *supra* n°655.

[1630] V. *supra* n°656.

[1631] Soit au titre d'une decision de justice (mandat de recherche, de comparution, d'amener ou d'arrêt, prévus à l'art. 122 du C. pr. pén.) soit au titre d'une procédure ouverte pour disparition inquiétante (C. pr. pén. art. 74-1).
Dans l'affaire de la disparition de Maëlys, à Grenoble, en 2017, le suspect de ce dossier s'est retrouvé mis en cause dans la disparition d'un militaire qui s'était produite plusieurs mois plus tôt. Le croisement de l'historique du bornage du téléphone du suspect avec le fichier des personnes recherchées est à l'origine de ce rebondissement.

[1632] Prévention des atteintes à la sécurité publique. V. *supra* n°710.

[1633] CNIL, délibération n°2009-355 du 11 juin 2009 portant avis sur un projet de décret en Conseil d'État portant création de l'application relative à la prévention des atteintes à la sécurité publique.

commission se réfère à la notion « d'activités publiques[1634] » qui peuvent conduire à l'inscription d'un individu dans le PASP et dont il est difficile de cerner ce que recouvre cette notion. La CNIL aurait également pu relever que « les personnes entretenant ou ayant entretenu des relations directes et non fortuites avec l'intéressé[1635] » peuvent être fichées, ce qui ouvre un périmètre démesurément vaste.

985. D'une manière générale, le rapport BATHO/BENISTI de 2011 dénonce le manque général de clarté des données nominatives susceptibles d'être collectées dans les traitements de données administratifs[1636], dont la majorité d'entre eux sont directement accessibles lors des enquêtes pénales[1637].

986. Le paroxysme du flou dans les données collectées. – En matière de flou dans les données collectées par les autorités publiques, les IMSI-catcher[1638] soulèvent des interrogations majeures. Leur fonctionnement tel que précédemment décrit[1639] montre qu'ils collectent une masse considérable de données à caractère personnel indirectement nominatives[1640]. Le législateur n'a pas éprouvé le besoin de déclarer un traitement de données à caractère personnel pour ce dispositif comme cela a été fait pour les écoutes téléphoniques[1641] ou la captation de données[1642], ce qui peut s'interpréter comme un réel malaise quant à la réalité de l'étendue des informations collectées. L'utilisation de ce dispositif par les autorités judiciaires concerne principalement les opérations importantes de trafic de drogue, où les criminels multiplient l'utilisation des cartes prépayées pour déjouer les placements sur écoute. L'IMSI-catcher sert alors aux enquêteurs à pouvoir intercepter les conversations téléphoniques échangées par un suspect à proximité de l'endroit où est placé l'appareil. Cette utilisation est particulièrement attentatoire au respect de la vie privée puisque, pour arriver à intercepter ces conversations, ce sont également les données nominatives de toutes les personnes se trouvant autour de l'IMSI-catcher qui sont enregistrées, en dehors de tout encadrement légal et règlementaire de l'utilisation et de la conservation de ces données.

[1634] C. séc. int. art. R236-12 7°.
[1635] C. séc. int. art. R236-12 9°. V. *supra* n°711.
[1636] *Op. cit.* p.35. BATHO Delphine et BENISTI Jacques-Alain, *rapport d'information sur la mise en œuvre des conclusions de la mission d'information sur les fichiers de police* : p. 48 et 49.
[1637] V. *supra* n°696.
[1638] C. pr. pén. art. 706-95-20
[1639] V. *supra* n°553.
[1640] Puisque toutes les données collectées sont rattachées à un numéro de carte SIM dont il est, dans la majorité des cas (les seules exceptions sont les cartes prépayées), possible de connaître le propriétaire.
[1641] Au travers de la PNIJ : v. *supra* n°687.
[1642] V. *supra* n°692.

987. Conclusion du paragraphe §1 : l'incohérence avec une spécialisation excessive des traitements judiciaires. – L'éparpillement des traitements judiciaires se veut protecteur des droits des personnes, en disséminant les données qui y sont enregistrées, évitant ainsi un fichage centralisé et complet de toutes les informations détenues. Or, ce sont précisément les données collectées qui rendent incohérentes cette vision protectrice de l'éparpillement des traitements auprès d'entités différentes. En effet, le besoin des autorités judiciaires en collecte de données est désormais tel, afin d'assurer l'efficacité de l'enquête pénale, que l'Etat se retrouve bloqué par une telle séparation, et y déroge dans les faits. Tout d'abord, des traitements regroupent des finalités différentes. Ensuite, l'étendue des données qui sont collectées dans les fichiers dépasse le périmètre annoncé. Enfin, certains traitements ont un périmètre flou, voire absent comme dans le cas des IMSI-catcher, et comportent des données dont il est impossible de cerner l'étendue ou leur utilisation.

988. Cette incohérence entre la finalité d'un traitement et les informations qui y sont enregistrées remonte à la création de celui-ci. Or, elle se poursuit lors de l'utilisation du traitement judiciaire, puisque le régime des traitements de données à caractère personnel n'est pas toujours respecté.

§2. L'incohérence avec le régime des traitements de données à caractère personnel

989. Une étanchéité très relative. – Les traitements judiciaires sont des traitements de données à caractère personnel pour lesquels un accès est directement prévu pour les autorités judiciaires en enquête pénale[1643]. Dès lors, ils sont soumis au régime des traitements de données à caractère personnel. Or, l'éparpillement des traitements judiciaires, qui induit un cloisonnement des données collectées, neutralise l'application des obligations qui incombent aux responsables des traitements judiciaires. Tout d'abord, cet éparpillement favorise, voire accentue, le défaut d'information des personnes fichées *(I)*. Ensuite, il nuit à la mise en œuvre d'un contrôle efficace des traitements judiciaires *(II)*.

[1643] V. *supra* n°968.

I – L'incohérence avec l'information de la personne fichée

990. L'information indispensable à l'exercice des autres droits. – Le prérequis pour qu'une personne puisse exercer son droit d'accès ou encore ses demandes de rectification[1644], est qu'elle sache que des informations nominatives la concernant ont été enregistrées[1645]. Ainsi, le fait que l'information des personnes fichées soit rarement prévue ou mal réalisée *(A)*, a inévitablement des conséquences négatives sur l'exercice potentiel des autres droits prévus pour les traitements de données à caractère personnel *(B)*.

A. Le défaut d'information

991. Le nécessaire équilibre entre la préservation de l'efficacité de l'enquête et le respect des libertés individuelles. – En matière de traitements judiciaires, il est légitime, afin de préserver l'efficacité de l'enquête, que l'information qui est prévue lors d'une collecte de données personnelles soit parfois neutralisée. La loi informatique et libertés[1646], dans sa nouvelle version issue de l'entrée en vigueur du RGPD[1647] et prenant en compte la directive européenne relative aux traitements judiciaires[1648], intègre cette possibilité au sein d'un principe de restriction plus large[1649]. Ce dernier peut s'appliquer à l'ensemble des obligations incombant normalement au responsable du traitement, notamment pour « éviter de gêner des enquêtes, des recherches ou des procédures

[1644] Dans le cas des traitements judiciaires, la rectification s'assimile souvent à la demande d'effacement.
[1645] BIANCHI Virginie, *L'effacement des fichiers ou le nouveau mythe de Sisyphe*, Dalloz, AJ Pénal 2007, p. 420 : « Encore faut-il que la personne fichée sache qu'elle l'est, ce que bien souvent elle découvre au détour d'un refus d'embauche, d'habilitation ou de visa ! En effet, bien peu de fichiers font l'objet d'une obligation systématique d'information de la personne fichée […]. »
[1646] Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par l'ordonnance du 12 décembre 2018
[1647] 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).
[1648] 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.
[1649] Le droit d'opposition au traitement est évidemment écarté : v. par ex. l'art. R53-21-25 relatif au REDEX (V. *supra* n°672.) : « Le droit d'opposition prévu au premier alinéa de l'article 38 [référence non mise à jour postérieurement à la refont de la loi informatique et libertés de 2018] de la même loi ne s'applique pas au présent traitement. » V. également l'art. R40-33 relatif au Traitement d'antécédents judiciaires.
V. également l'art. 7 du décret n°2015-1700 du 18 décembre 2015 relatif à la mise en œuvre de traitements de données informatiques captées en application de l'article 706-102-1 du code de procédure pénale. C'est non seulement le droit d'opposition mais également le droit d'information qui sont, fort logiquement (puisque l'on est dans le cadre d'une mesure de surveillance : v. *supra* n°692.) écartés : « Le droit d'information et le droit d'opposition prévus aux articles 32 et 38 de la loi du 6 janvier 1978 [même remarque que pour l'article R53-21-25, ci-dessus] susvisée ne s'appliquent pas au présent traitement. »

administratives ou judiciaires[1650] ». En revanche, dès lors que l'enquête est terminée ou qu'une personne a fait l'objet d'une collecte de données au sein d'une enquête pénale, sans être impliquée dans des faits délictueux ou criminels, il serait légitime que le devoir d'information s'applique.

992. Des personnes ayant fait l'objet d'une collecte de données non-informées. – Sur ce point, le cas de l'IMSI-catcher qui vient d'être évoqué[1651] est représentatif. Certes, le principal problème avec cet acte d'investigation numérique est que les données interceptées et enregistrées par ce dispositif ne font l'objet d'aucun traitement de données à caractère personnel dument déclaré. Néanmoins, en faisant abstraction de cette difficulté originelle, l'IMSI-cacher illustre parfaitement la non-information d'une personne totalement étrangère à des faits répréhensibles, mais s'étant trouvée dans la zone d'intervention du dispositif et ayant donc fait l'objet d'une collecte et d'un enregistrement de données par les autorités judiciaires. L'absence d'information est d'autant plus sensible que l'IMSI-catcher collecte non seulement les données d'identification des appareils utilisant des lignes téléphoniques mobiles, mais également la localisation des utilisateurs et, potentiellement, les contenus des données ou des conversations qui transitent via la ligne[1652].

993. Le modèle Allemand en matière d'information. – Sur ce point, le droit pénal Allemand est rigoureux car il est explicitement prévu qu'une personne ayant fait l'objet d'une collecte de données lors d'une enquête en soit informée au plus tard à la clôture des investigations[1653]. Ce cadre légal est cohérent avec la position de la CJUE[1654].

En droit français, une telle rigueur n'existe pas car, hormis quelques rares cas où l'individu fiché est informé au titre de dispositions prévues par un texte, la situation la plus fréquente est celle décrite avec les IMSI-catcher où les personnes ayant fait l'objet d'une collecte de données ne le savent pas. Cette situation s'oppose à une récente décision de la Cour de Justice de l'Union Européenne[1655].

[1650] *Ibid.* Loi informatique et libertés, art. 107.
[1651] V. *supra* n°986.
[1652] V. *supra* n°563.
[1653] *Op. cit.* p.35. JAEGER Christian, *Enquêtes secrètes, perquisitions en ligne et conservation des données en Allemagne : un équilibre entre les intérêts de la poursuite pénale et les garanties de l'Etat de droit,* Colloque sur « les investigations numériques en procédure pénale comparée » du 5 mai 2017 au Pôle Juridique et Judiciaire de Bordeaux.
[1654] CJUE 6 oct. 2015, aff. C-362/14 « Schrems ».
[1655] CJUE, 21 déc. 2016, aff. jtes C-203/15 et C-698/15 « Tele2 Sverige et Watson »

994. L'information par la notification d'obligations. – Une personne est nécessairement informée lorsque l'inscription dans un fichier est assortie d'obligations pour l'individu fiché. C'est essentiellement le cas avec le fichier judiciaire national automatisé des auteurs d'infractions terroristes[1656] et le fichier national automatisé des auteurs d'infractions sexuelles ou violentes[1657]. Ici, un ensemble de dispositions décrivent les « obligations incombant à la personne inscrite dans le fichier[1658] ». Il est trivial d'expliquer qu'évidemment, pour qu'une personne puisse appliquer les obligations qui lui sont imposées[1659], il doit préalablement lui être notifié qu'elle est inscrite dans la base de données concernée. Hormis dans ce type de situation où l'information est obligatoirement réalisée pour que la personne fichée puisse exécuter les obligations qui lui incombent, l'information est rarement réalisée.

995. Le cas du Traitement d'Antécédents Judiciaires (TAJ). – Comme expliqué précédemment, le TAJ est l'outil de travail de base des enquêteurs[1660], et contient donc une richesse d'information colossale. Ainsi, il comportait en 2013 12,2 millions de fiches de personnes mises en cause[1661].

996. L'article 230-8 du Code de procédure pénale, qui porte les dispositions principales encadrant le TAJ, a connu plusieurs modifications importantes en peu de temps. Après quelques retouches introduites par la loi du 3 juin 2016[1662], dont l'objectif était principalement de durcir les conditions d'effacement des informations personnelles, il a fait l'objet d'une déclaration partielle d'inconstitutionnalité[1663]. « Le Conseil a jugé que ces dispositions portaient une atteinte disproportionnée au droit au respect de la vie

---

DANIS-FATÔME Anne, *Lutte contre le terrorisme - La protection des données personnelles résiste à la surveillance générale qu'imposerait la lutte contre le terrorisme,* LexisNexis, Communication Commerce Electronique n°4, avril 2020.

[1656] V. *supra* n°667.

[1657] *Ibid.*

[1658] V. resp. les art. R50-43 à R50-50 pour le terrorisme et R53-8-13 à R53-8-21 pour les infractions sexuelles et violentes.
THOMAS-TAILLANDIER Delphine, *Le nouveau fichier national des auteurs d'infractions terroristes*, Dalloz AJ pénal 2015 p.523 : « […] le FIJAIT est un outil contraignant pour la personne qui y est inscrite. En effet, le législateur a choisi d'en faire une mesure de police restreignant la liberté d'aller et venir des individus identifiés comme terroristes. […] toute personne fichée devra respecter un ensemble d'obligations de justification et de présentation […]. »

[1659] *A minima*, informer de tout changement d'adresse et, suivant la décision judiciaire, des obligations de présentation.

[1660] V. *supra* n°643.

[1661] CNIL, *Conclusions du contrôle des fichiers d'antécédents du ministère de l'intérieur,* Rapport adopté en séance plénière le 13 juin 2013, p. 6.

[1662] Loi du n°2016-731 du 3 juin 2016. *Op. cit.* p.35.

[1663] Cons. const, décision n°2017-670 QPC du 27 octobre 2017.

privée, parce qu'elles privaient les personnes mises en cause dans une procédure pénale, autres que celles ayant fait l'objet d'une décision d'acquittement, de relaxe, de non-lieu ou de classement sans suite, de toute possibilité d'obtenir l'effacement de leurs données personnelles inscrites dans ce fichier[1664] ». La loi du 20 juin 2018, adaptant le droit français au RGPD[1665] ainsi qu'à la directive relative aux traitements judiciaires[1666] a alors modifié en profondeur cet article[1667].

997. Néanmoins, l'information d'une personne fichée reste la grande oubliée de l'ensemble de ces modifications et aucun cadre légal précis n'a été posé en la matière. Le seul cas où l'information d'un individu fiché est explicitement prévue, est lorsqu'il a été mis en cause au stade de l'enquête (et que donc des informations en ce sens ont été saisies dans le TAJ) et que la procédure se solde par « une décision de relaxe ou d'acquittement devenue définitive[1668] ». Dans ce cas, les données personnelles en question doivent, théoriquement, être effacées, sauf « si le procureur de la République en prescrit le maintien[1669] », auquel cas le procureur est tenu d'en aviser la personne concernée. Cette dernière peut alors exercer un certain nombre de recours contre la décision du procureur.

998. Une absence d'information dans les faits. – Le TAJ joue un rôle central dans le travail de police judiciaire, et il n'existe quasiment aucune obligation d'informer une personne ayant fait l'objet d'un enregistrement de données personnelles dans ce traitement. Dès lors, pourquoi les policiers ou les gendarmes s'imposeraient-ils d'informer systématiquement un individu lorsqu'ils ont enregistré des informations le concernant ?

999. L'effet exponentiel du défaut d'information. – La multiplication des traitements accentue considérablement cette absence d'information pour les personnes concernées puisque, conjointement au TAJ, un individu peut se voir fiché, pour les mêmes

---

[1664] ROUMIER William, *Régime d'effacement des données du fichier d'antécédents judiciaires*, JurisClasseur Droit pénal n°9, Septembre 2018.
[1665] 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).
[1666] 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.
[1667] Loi n°2018-493 du 20 juin 2018 relative à la protection des données personnelles, art. 36.
[1668] C. pr. pén. art. 230-8.
[1669] *Ibid.*

faits, dans un nombre importants d'autres traitements. En effet, les autorités publiques peuvent, *a minima*, enrichir le fichier des empreintes digitales et plusieurs fichiers liés à la sécurité publique[1670]. De plus, le juge peut ordonner l'enregistrement de données dans des traitements spécialisés avant même une éventuelle condamnation[1671].

1000. Conclusion du sous-paragraphe A : le défaut d'information. – Hormis des traitements associés à une mesure de surveillance comme la captation des données où le devoir d'information est explicitement écarté, c'est le silence de la loi qui prévaut en matière de traitements judiciaires sur ce point. Ainsi, une personne dont le nom apparaît dans une procédure, quel qu'en soit le stade, peut se voir fichée dans plusieurs traitements judiciaires sans qu'elle en ait connaissance. Cette difficulté est directement liée à l'éparpillement et la multiplication des traitements judiciaires, car la probabilité est faible pour qu'une personne fichée ait connaissance de l'existence même des fichiers dans lesquels des données la concernant sont enregistrées.

1001. Ce défaut d'information a pour effet de neutraliser l'exercice d'autres droits normalement prévus en matière de protection des données personnelles.

B. Les conséquences du défaut d'information

1002. Les conséquences des déficiences de l'information. – Le défaut d'information a évidemment des conséquences sur le possible exercice des autres droits théoriquement applicables aux traitements de données à caractère personnel, à savoir le droit d'accès, le droit de rectification et d'effacement. En matière de traitements judiciaires, l'effacement correspond parfaitement à l'expression « droit à l'oubli » qui est souvent employée[1672]. Si une personne fichée ne reçoit pas une information précise et officielle, cela hypothèque nécessairement l'exercice de ses autres droits[1673]. Le fait de ne pas exercer ces autres droits, dont principalement le droit d'accès et de rectification, a pour effet de nuire indirectement à la qualité des données. En effet, la personne concernée par les données est celle qui a le plus d'intérêt à ce que les informations enregistrées soient à jour ou

[1670] Par ex. le PASP et l'EASP - V. *supra* n°711.
[1671] Par ex. le fichier judiciaire national automatisé des auteurs d'infractions sexuelles ou violentes, le fichier national automatisé des empreintes génétiques, etc.
[1672] V. par ex. : Revue Lamy Droit de l'immatériel, 1er août 2017, *Interrogations sur la portée territoriale du droit au déréférencement*, n°140.
[1673] VIBRAC Geoffrey, *Les fichiers à l'épreuve de nouveaux droits effectifs pour les personnes ?*, Dalloz AJ pénal 2018 p.564.

effacées. Ainsi, si elle n'exerce pas ses autres droits par méconnaissance, cela neutralise un potentiel contrôle des mises à jour de ses données qui pourrait être essentiel.

1003. Une évolution favorable du droit d'accès. – Le droit d'accès est celui qui fait logiquement suite à l'information puisque, dès lors que l'on sait que l'on est fiché dans un traitement judiciaire, il est logique d'avoir envie d'en connaître le contenu. La loi informatique et libertés issue des modifications découlant de l'entrée en vigueur du RGPD[1674] et de la directive relative aux traitements judiciaires[1675] retranscrit parfaitement cette logique, puisque « la personne concernée a le droit d'obtenir […] la confirmation que des données […] la concernant sont ou ne sont pas traités et, lorsqu'elles le sont, le droit d'accéder auxdites données […][1676] ».

1004. Néanmoins, il faudra certainement un moment pour que cette disposition devienne effective. En l'état actuel, le droit d'accès est particulièrement complexe dans ses modalités d'exercice. Il est parfois direct, comme dans le cas du fichier des empreintes digitales[1677], ou celui des empreintes génétiques[1678], parfois indirect via la CNIL[1679], voire un mélange des deux comme avec le fichier des personnes recherchées qui, en fonction des données auxquelles on souhaite avoir accès, renvoi vers la direction centrale de la police judiciaire de ministère intérieur ou vers la CNIL[1680].

1005. L'officialisation du droit de rectification. – La loi informatique et libertés dans sa nouvelle version impose une obligation de rectification aux « autorités compétentes[1681] ». Mais elle entérine également un droit de rectification pour les personnes faisant l'objet d'un fichage dans un fichier judiciaire[1682]. Actuellement, le droit

[1674] *Op. cit.* p.35
[1675] *Ibid.*
[1676] Loi informatique et libertés modifiée par l'ordonnance du 12 décembre 2018, art. 105.
[1677] Décret n°87-249 du 8 avril 1987 relatif au fichier automatisé des empreintes digitales géré par le ministère de l'intérieur, art. 6 : « Les droits d'accès et de rectification prévus par les articles 39 et 40 de la loi n°78-17 du 6 janvier 1978 s'exercent auprès du directeur central de la police judiciaire au ministère de l'intérieur, place Beauvau, Paris (8e). »
[1678] C. pr. pén. art. R53-15 : « Le droit d'accès prévu […] s'exerce auprès du directeur central de la police judiciaire au ministère de l'intérieur. »
[1679] V. par. ex. le traitement automatisé de contrôle des données signalétiques des véhicules (Arrêté du 18 mai 2009), art. 6 : « Le droit d'accès et de rectification s'exerce de manière indirecte auprès de la Commission nationale de l'informatique et des libertés dans les conditions prévues à l'article 41 de la loi du 6 janvier 1978 susvisée. »
[1680] Décret n°2010-569 du 28 mai 2010 relatif au fichier des personnes recherchées, art. 9.
[1681] Loi informatique et libertés modifiée par l'ordonnance du 12 décembre 2018, art. 97.
[1682] *Ibid.*, art. 106.

de rectification est souvent traité conjointement au droit d'accès[1683] alors qu'il est pourtant beaucoup plus proche de l'effacement. En effet, il est évident qu'un individu fiché exerce son droit de rectification lorsque les données dont il demande la modification lui seront plus favorables, et donc se rapproche en ce sens de l'effacement. Or, l'éparpillement et la multiplication des traitements judiciaires nuit une nouvelle fois aux personnes qui souhaitent faire une demande de rectification et d'effacement, car il n'existe aucun régime homogène pour cela d'un traitement à un autre. Les différents fichiers prévoient une (voire des) procédure(s) pour pouvoir exercer ces droits-là. La complexité et le manque de clarté de ces procédures transparaissent sur plusieurs points, et perdurent depuis de nombreuses années[1684].

1006. En premier lieu, une multitude de régimes dérogatoires sur les durées de conservation « de base[1685] » a pour effet de neutraliser les cas d'effacements normalement prévus[1686].

1007. En deuxième lieu, il existe une sorte de renversement de la charge de la mise en œuvre de la procédure d'effacement[1687].

1008. En troisième lieu, comme vu précédemment[1688], plusieurs structures sont parfois compétentes pour recevoir le droit de rectification qui serait exercé par un individu pour un même traitement.

1009. En quatrième et dernier lieu, les traitements judiciaires prévoient le plus souvent que le droit de rectification peut être exercé auprès du responsable du traitement, à savoir

---

[1683] V. par ex. le traitement automatisé de contrôle des données signalétiques des véhicules (Arrêté du 18 mai 2009), *op. cit.* : « Le droit d'accès et de rectification […] » ou le décret n° 2010-569 du 28 mai 2010 relatif au fichier des personnes recherchées, art. 9 : « […] les droits d'accès et de rectification […] ».

[1684] BAUER Alain, *Rapport public - Fichiers de police et de gendarmerie : comment améliorer leur contrôle et leur gestion ?*, 27 nov. 2006, p. 116 : « Une des difficultés est que le public distingue souvent mal l'exercice des droits d'accès aux fichiers de police […], de l'exercice d'un recours […]. »

[1685] Les exemples les plus notables sont Cassiopée (v. *supra* n°623.) et le fichier national des empreintes génétiques (v. *supra* n°661.). Pour Cassiopée, l'article R15-33-66-7 cumule plusieurs régimes dérogatoires venant allonger la durée de 10 ans, avec des dispositions venant modifier le point de départ de ce délai de conservation. Il en est de même pour le fichier des empreintes génétiques (C. pr. pén. art. R53-11).

[1686] V. par ex. : 1 - Le casier judiciaire : l'art. 769 du C. pr. pén. prévoit des effacements de fiches mais assortis d'une multiplicité de régimes dérogatoires (voir le champ lexical composé de « sauf », « toutefois », « si », etc), ce qui rend la mesure d'une complexité redoutable.

2 - Le fichier des antécédents avec l'art. 230-8 du C. pr. pén. : « En cas de décision de relaxe ou d'acquittement devenue définitive, les données personnelles concernant les personnes mises en cause sont effacées, sauf si le procureur de la République en prescrit le maintien […] ». Il s'ensuit des conditions qui, dans les faits, offrent au Procureur la possibilité de neutraliser l'effacement des données (V. *supra* n°995.).

[1687] Fichier des empreintes génétiques : C. pr. pén. art. R53-13-1 à R53-13-6 qui encadrent la demande d'effacement que formulerait l'intéressé.

[1688] V. *supra* n°1004.

dans la majorité des cas le ministère de l'intérieur[1689]. Il est particulièrement regrettable qu'aucun correspondant ne soit clairement énoncé, car le fait d'écrire au ministère de l'intérieur (ou à des services aussi vastes que la « direction centrale de la police judiciaire[1690] ») pour exercer son droit de rectification est totalement incohérent. Un correspondant pourrait, en effet, être désigné, certes de manière non nominative, mais au travers de sa fonction[1691] ou, à tout le moins, au travers d'un service précis.

1010. Les spécificités de l'effacement. – En matière d'effacement, il existe, pour certains traitements, une procédure qui ouvre le droit à la personne fichée d'en faire la demande, avant que la durée légale de conservation soit atteinte. Il s'agit donc de l'ouverture d'un droit à l'effacement qui est une forme particulière du droit de rectification. C'est le cas pour le fichier des empreintes génétiques[1692] ou des empreintes digitales[1693]. Un cas pratique révèle qu'une personne, initialement mise en cause dans un dossier de vol, et dont les empreintes digitales ont été enregistrées, a précisément procédé à une demande d'effacement de ses empreintes dans ledit fichier selon la procédure en vigueur, après qu'un classement sans suite ait été prononcé. Le refus des différentes instances saisies selon la procédure[1694] s'est soldé par une condamnation de la France par la CEDH[1695], au motif d'avoir maintenu des informations dans le fichier, malgré l'abandon des poursuites contre un individu, dans un contexte où la durée de conservation était longue. Ces deux éléments pris ensemble ont été déclarés, par la CEDH, disproportionnés par rapport aux intérêts publics qui étaient en jeux. Cet arrêt ne faisait que réaffirmer des décisions antérieures[1696].

1011. Le cas du traitement d'antécédents judiciaires. – Une nouvelle fois il est nécessaire de s'intéresser au cas particulier du TAJ en raison du rôle essentiel de celui-ci et de sa richesse d'informations[1697]. Dans sa version issue de la loi du 20 juin 2018[1698],

---

[1689] V. annexe 1 : sur l'ensemble des fiches, le responsable du traitement est énoncé.
[1690] Cas du fichier des personnes recherchées : art. 9 du décret n°2010-569 du 28 mai 2010 relatif au fichier des personnes recherchées.
[1691] Par exemple, la loi informatique et libertés dans sa nouvelle version impose, dans son article 103, aux responsables des traitements judiciaires de désigner un DPO (délégué à la protection des données).
[1692] V. C. pr. pén. art. 706-54 al. 2.
[1693] *Op. cit.* Décret n°87-249 du 8 avril 1987, art. 3.
[1694] Resp. le procureur de la République, le JLD, le président de la chambre d'instruction et la Cour de cassation.
[1695] CEDH 18 avril 2013 M. K. c. France n°19522/09. CEDH 6 juin 2006 Segerstedt-Wiberg c. Suède.
[1696] CEDH 4 dec. 2008 S. et Marper c. Royaume Uni.
[1697] V. *supra* n°995.
[1698] Loi n°2018-493 du 20 juin 2018, *op. cit.* p.35

un droit d'effacement est ouvert à « la personne concernée » pour les données[1699]. Dans les faits, la personne concernée ne peut exercer ce droit que lorsqu'elle est mise hors de cause[1700] ou que son éventuelle condamnation antérieure a été effacée du « bulletin n°2 de son Casier judiciaire ». Il est particulièrement incohérent qu'une personne ait à demander que ses données soient effacées lorsqu'elle est définitivement mise hors de cause, alors que le procureur est censé le faire spontanément, sauf s'il en décide le contraire[1701]. Dans ce cas, comme précédemment expliqué, il doit en informer la personne concernée[1702]. Le seul fait de prévoir la possibilité que la personne concernée puisse demander que ses données soient effacées, fait naître la crainte que, dans les faits, le procureur ne procède que rarement à l'effacement de sa propre initiative.

1012. Une simple « mention » en contrepartie de la neutralisation du droit à l'effacement. – Lorsque le procureur prescrit le maintien des données d'une personne malgré une « décision de non-lieu ou d'acquittement devenue définitive », ces données « font l'objet d'une mention ». Cette mention a pour objectif de bloquer l'accès à ces informations maintenues, en cas de consultation du TAJ « dans le cadre des enquêtes administratives ». La fragilité d'une telle procédure est évidente. D'une part, la protection des droits de la personne concernée repose intégralement sur une sorte de case à cocher dans le TAJ sans que, bien évidemment, cette personne ne dispose du moindre moyen pour s'assurer que cette action ait bien été réalisée. D'autre part, le TAJ est un traitement entièrement géré par les officiers de police judiciaire, et non par des juges indépendants, ce qui accentue la fragilité de la protection des droits de la personne dont les informations sont maintenues dans le TAJ. En effet, les policiers ou les gendarmes peuvent résister à la demande d'inscription de la mention en ne cochant pas la case correspondante.

[1699] C. pr. pén. art. 230-8, al. premier.

[1700] Ce qui s'inscrit dans la continuité du régime antérieur à 2018. V. Trib. admin. Montreuil, 8ème ch., 27 mai 2016, n°1500040 : « […] que toutefois, en l'absence de demande relative à l'effacement d'une décision de relaxe, d'acquittement, de non-lieu ou de classement sans suite, les stipulations de cet article sont inopérantes à l'encontre d'une décision par laquelle le procureur de la République territorialement compétent refuse de faire droit à cette demande. »
V. eg. CAA Marseille, 7ème ch., 30 mars 2018, n° 16MA02755 : un simple rappel à la loi neutralise la possibilité de demande d'effacement.

[1701] BUISSON Jacques, *Preuve – Moyens de la preuve*, Dalloz Répertoire de droit pénal et de procédure pénale, Octobre 2019 : « Il peut paraître hétérodoxe que le procureur, hiérarchiquement soumis au ministre de la Justice, puisse s'opposer à un tel effacement, sans que soit corrélativement aménagé un recours à l'encontre de cette décision. »

[1702] V. *supra* n°997.

1013. Le droit à ce que les données conservées soient exactes[1703]. – Le droit de rectification trouve son prolongement dans la mise à jour des fichiers puisqu'il s'agit, dans ses effets, de son équivalent du côté du responsable du traitement. A la différence du droit d'accès ou de rectification, la mise à jour des fichiers de police n'est pas un droit que la personne concernée exerce directement. Il s'agit d'un droit *in abstracto* pour toutes les personnes fichées, que les données les concernant soient exactes, complètes et à jour. Ce principe est désormais inscrit dans la nouvelle version de la loi informatique et libertés[1704].

1014. En matière de traitements de données judiciaires, la mise à jour est plus importante que le droit de rectification donné à une personne car ce dernier est fortement encadré en raison de la finalité même de ces fichiers. En revanche, la mise à jour, qui est censée incomber aux autorités publiques, est primordiale. Les conséquences des informations erronées dont, tout particulièrement, celles non effacées alors qu'elles devraient l'être, peuvent être très importantes pour un individu[1705]. Les difficultés de mise à jour sont dénoncées depuis plusieurs années. Dès 2009, la CNIL, dans un rapport remis au premier ministre sur le STIC, relevait « l'absence quasi-systématique de transmission par les parquets des suites judiciaires nécessaires à la mise à jour du STIC[1706] ».

1015. Le rapport poursuit en expliquant les conséquences des informations erronées puisque « la consultation de ces fichiers d'antécédents est également effectuée pour l'instruction des demandes d'acquisition de la nationalité française, la délivrance et le renouvellement des titres relatifs à l'entrée et au séjour des étrangers, […] et à l'occasion de la présentation de certains concours de la fonction publique […] ». Les fichiers de police sont également consultés pour d'autres emplois[1707]. Au demeurant, il est inquiétant que le rapport de la CNIL de 2013 sur le même sujet, réitère les mêmes problèmes[1708].

[1703] ALLAIN Emmanuelle, *Fichiers d'antécédents : un rapport préoccupant*, Dalloz AJ pénal 2013 p.370 : « S'agissant de la fiabilité des données, les conclusions sont alarmantes […]. »

[1704] Loi informatique et libertés art. 97.

[1705] GAUTRON Virginie, *Usages et mésusages des fichiers de police : la sécurité contre la sureté ?* Dalloz AJ Pénal 2010 p.266 : « ces consultations [aux fins d'enquêtes de moralité] occasionnent parfois des licenciements ou des refus d'embauche injustifiés ».

[1706] CNIL, *Conclusions du contrôle du système de traitement des infractions constatées (STIC),* Rapport remis au Premier ministre le 20 janvier 2009 : p. 17 et 25.

[1707] GAUTRON Virginie, *Fichiers de police – Réglementation française*, Dalloz, Répertoire de droit pénal et de procédure pénale, mars 2019, §2. Contentieux des décisions administratives fondées sur la consultation des fichiers de police : « Les juridictions administratives se prononcent fréquemment sur les recours exercés par différents professionnels (agents privés de sécurité, policiers municipaux, etc.) suite à des refus d'agréments opposés après la consultation de certains fichiers de police. »

[1708] CNIL, *Conclusions du contrôle des fichiers d'antécédents du ministère de l'intérieur,* Rapport adopté en séance plénière le 13 juin 2013, p.7 : « les défaillances observées en 2009 n'ont pas connu

1016. Les spécialistes de la sécurité publique confirment que « les dysfonctionnements sont d'abord liés à l'absence de transmission régulière par les parquets des suites judiciaires favorables au gestionnaire[1709] […] ». Mais, pire, même lorsque les effacements sont demandés par le Parquet, il n'est pas rare que ceux-ci ne soient pas effectués par la Police[1710]. De plus, les officiers de police judiciaire sont des travailleurs comme les autres dans leur comportement avec leurs outils numériques et, à ce titre, ils appliquent l'adage « on ne sait jamais, cela peut toujours servir ». A maintes reprises, les deux rapports émis par Delphine BATHO et Jacques-Alain BENISTI dénoncent l'inexactitude des données contenues dans les fichiers judiciaires[1711].

1017. Dans des cas extrêmes, la mise à jour est pratiquement impossible. Ce sera le cas lorsque les policiers ou les gendarmes créent, soit dans un fichier en local sur leur ordinateur de bureau, soit en utilisant la « zone poubelle[1712] » du traitement de données STIC[1713] qui a pour propriété technique de rester locale au poste de travail de l'officier de police judiciaire. Dans les deux cas ces bases de données se situent en dehors de tout cadre légal et, par voie de conséquence, la probabilité qu'elles ne soient pas mises à jour est importante.

1018. Une mise à jour fortement complexifiée par la multiplication des traitements judiciaires. – L'éparpillement des traitements judiciaires complexifie énormément la mise à jour des fichiers. En effet, il est difficile de répercuter la consigne de modification ou d'effacement sur l'ensemble des traitements susceptibles d'être concernés. Il s'agit là d'une des causes principales des défaillances dans la mise à jour de ces fichiers dont les deux conséquences majeures sont le nombre important d'informations erronées et le non-effacement de données y compris lorsque celui-ci est de droit.

---

d'améliorations notables […] quant à la mise à jour des données par les procureurs de la République chargés de faire connaître au ministère de l'intérieur certaines suites judiciaires. »

[1709] *Op. cit.* p.35, BAUER Alain et SOULLEZ Christophe, *Les fichiers de police et de gendarmerie.*

[1710] *Op. cit.* p.35, BATHO Delphine et BENISTI Jacques-Alain, *rapport d'information sur les fichiers de police,* Commission des lois constitutionnelles, de la législation et de l'administration générale de la République de l'Assemblée Nationale, enregistré le 24 mars 2009 : p. 127.

[1711] *Op. cit.* p.35, BATHO Delphine et BENISTI Jacques-Alain, *rapport d'information sur la mise en œuvre des conclusions de la mission d'information sur les fichiers de police,* Commission des lois constitutionnelles, de la législation et de l'administration générale de la République de l'Assemblée Nationale, enregistré le 21 décembre 2011 : v. par ex p.70 et s. et p.77 et s. : « Le stock de données erronées demeure une préoccupation majeure. »

V. encore p. 51 sur la conséquence des inexactitudes des informations contenues dans les fichiers.

[1712] *Ibid*, CNIL, *Conclusions du contrôle du système de traitement des infractions constatées (STIC),* p.7 et s.

[1713] V. *infra* n°644.

1019. Toutefois, les informations erronées peuvent également être le fait d'une erreur de saisie dès la création d'une fiche personnelle[1714]. Par exemple, dans le cas du TAJ, c'est un simple code composé d'une lettre qui permet de distinguer les personnes mises en cause, les témoins et les victimes. En conséquence, une simple erreur de saisie dans un code (« E » au lieu de « C ») peut être lourd de conséquences pour la victime qui se retrouve indument identifiée comme mise en cause pour une simple erreur de saisie dans un code[1715]. Par ailleurs, ce classement trouve rapidement ses limites quant à l'effectivité de la protection, car il suffit que le nom de la victime soit explicitement saisi dans la fiche de la personne mise en cause (dans la rubrique description des faits) pour que le nom de la victime ressorte alors qu'il ne devrait pas[1716].

1020. Les effets d'une erreur de manipulation des paramètres du TAJ serait identique si « la mention[1717] », qui permet de neutraliser la consultation à des fins administratives lorsque le procureur a prescrit le maintien de données dont l'effacement est normalement dû, n'est pas cochée ou n'est pas activée pour l'ensemble des informations concernées.

1021. Conclusion du sous-paragraphe I : l'incohérence avec l'information de la personne fichée. – L'éparpillement et la multiplication des traitements judiciaires nuisent au respect des règles de la protection des données personnelles. En effet, ils accentuent, notamment, l'absence d'information de la personne fichée en accumulant les difficultés pour elle d'exercer ses droits d'accès, de rectification ou d'effacement.

1022. Certes, il est prévu par la loi de pouvoir neutraliser les droits incombant au responsable du traitement lorsqu'il s'agit de traitements judiciaires, afin de ne pas nuire à l'enquête. Néanmoins, il serait légitime qu'une personne ayant fait l'objet d'une saisie d'informations nominatives dans un traitement judiciaire en soit informé, au plus tard à la fin de la procédure ayant conduit à la collecte de données. Or, cette information est rarement prévue. Cette absence d'information, préjudiciable en elle-même, est alors amplifiée par l'effet négatif de l'éparpillement des traitements judiciaires. Le nombre important de fichiers dans lesquels cette personne peut se voir identifiée, accentue l'absence d'information initiale. En effet, la multiplication de traitements judiciaires et

[1714] PARIS Didier et MOREL-A-L'HUISSIER Pierre, *Rapport d'information sur les fichiers mis à la disposition des forces de sécurité*, déposé et enregistré à l'Assemblée nationale le 17 oct. 2018, p. 35.
[1715] *Ibid,* CNIL, *Conclusions du contrôle du système de traitement des infractions constatées (STIC),* p.7 du rapport.
[1716] Les art. R40-29 et R40-29-1 du C. pr. pén. disposent que les informations relatives aux victimes ne doivent pas être accessibles pour certaines consultations.
[1717] V. *supra* n°1012.

leur dissémination auprès d'entités différentes lui ôtent toute possibilité d'exercer ses droits d'accès, de rectification et d'effacement lorsqu'il est prévu, puisqu'elle ne sait pas dans quels fichiers elle peut être fichée. Il y a là une incohérence majeure entre la protection des données personnelles et l'éparpillement des traitements judiciaires.

1023. De plus, la mise à jour, légalement prévue, qui incombe aux autorités judiciaires, n'est pas systématiquement réalisée. Dès lors, l'absence d'information a les mêmes conséquences puisque la personne fichée est dans l'incapacité de vérifier que la mise à jour a bien été réalisée.

1024. C'est alors que les contrôles des autorités publiques sur les traitements judiciaires s'avéreraient indispensables. Malheureusement, ceux-ci souffrent de la même incohérence due à l'éparpillement des fichiers.

II – L'incohérence avec un contrôle effectif

1025. Des contrôles de fichiers hautement théoriques. – Le non-respect des obligations incombant au responsable d'un traitement judiciaire est inextricablement associé à l'éparpillement et à la multiplication des fichiers. L'information ne circule que difficilement entre des services différents, souvent rattachés à des autorités hiérarchiques distinctes, voire des ministères différents[1718].

1026. Dans ce contexte, les contrôles des fichiers devraient permettre de prévenir et de pallier les dysfonctionnements, essentiellement pour les mises à jour et les rectifications des données. Pour ce faire, les contrôles devraient vérifier la qualité des informations enregistrées, ainsi que la prise en compte des demandes de modifications émanant des autorités judiciaires. Or, certains auteurs n'hésitent pas à affirmer que « les contrôles et garanties offerts s'avèrent plus que théoriques » et que « la faiblesse des contrôles institués portent indéniablement atteinte aux libertés fondamentales[1719] ».

1027. Une pluralité de régimes hétérogènes. – En effet, bien qu'il soit impossible de dégager une règle tant les modalités des contrôles de la mise en œuvre des traitements judiciaires sont spécifiques à chaque texte à l'origine de leur création, il se dégage que beaucoup de fichiers sont placés sous le contrôle d'un magistrat du parquet[1720] sachant

[1718] Ministère de l'intérieur et Ministère de la justice.
[1719] *Ibid*, GAUTRON Virginie, *Usages et mésusages des fichiers de police : la sécurité contre la sureté ?*
[1720] Ex. : fichier des empreintes génétiques, C. pr. pén. art. R53-9.

que, pour les plus récents d'entre eux, les pouvoirs publics ont ajouté une précision : celui-ci est placé hors hiérarchie[1721]. Pour les fichiers que l'on peut qualifier de hautement sensibles, le rôle central du service du Casier judiciaire a déjà été évoqué[1722]. On retrouve celui-ci dans le contrôle de ces traitements qui est confié au « magistrat dirigeant le service du Casier judiciaire[1723] ». Pour tous les traitements qui sont créés par un simple arrêté, aucun contrôle n'est globalement énoncé[1724]. Dans le cas des traitements de données administratifs pour lesquels un accès est prévu pour les enquêteurs[1725], très peu de contrôles sont explicités. Tout au plus, dans le cas du fichier relatif à « la prévention des atteintes à la sécurité publique (PASP) » et celui pour la « gestion de l'information et prévention des atteintes à la sécurité publique[1726] » des référents issus du Conseil d'Etat sont nommés pour émettre des préconisations et s'assurer de l'effacement[1727].

1028. Le modèle efficace de la PNIJ. – Seule la PNIJ[1728] peut être prise pour modèle puisqu'elle est placée sous la responsabilité d'une personne désignée, assistée par un comité de cinq membres[1729]. La PNIJ possède une autre spécificité positive, qui peut être vue comme une sorte d'effacement provisoire des données : la mise sous scellés numériques[1730]. Celle-ci revient à rendre impossible leur exploitation. Elle est identique dans ses effets à un effacement, à la différence qu'il est possible de revenir en arrière en brisant les scellés, afin de pouvoir reprendre l'analyse des données ou de procéder à une contre-expertise.

Le rôle de ce magistrat est issu de la loi n°2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure (dite LOPPSI II). V. RIBEYRE Cédric, *LOPPSI II : de nouvelles règles au service de la répression*, LexisNexis Droit pénal n°7-8, Juillet 2011, étude 10.

[1721] C'est le cas pour les logiciels de rapprochement judiciaire (C. pr. pén art. R40-41) et pour les fichiers d'analyse sérielle (art. R. 40-37) : « La mise en œuvre et la mise à jour des traitements sont contrôlées par un magistrat du parquet hors hiérarchie, désigné pour trois ans par arrêté du garde des sceaux, ministre de la justice, et assisté par un comité composé de trois membres nommés dans les mêmes conditions. »

[1722] V. *supra* n°641. et 668.

[1723] V. le fichier judiciaire national automatisé des auteurs d'infractions sexuelles ou violentes (C. pr. pén. art. R53-8-1), le fichier national automatisé des auteurs d'infractions terroristes (art. R50-30) ou encore le REDEX (art. R53-21-1).

[1724] V. par ex. les traitements automatisés de contrôle des données signalétiques des véhicules, le fichier des objets et des véhicules signalés (FOVeS), etc.

[1725] V. *supra* n°696.

[1726] V. *supra* n°709.

[1727] V. resp. C. séc. int. art. R236-15 et R236-26.

[1728] Qui présente la caractéristique d'être à la fois une structure pour la mise en œuvre opérationnelle des écoutes téléphoniques et un traitement de données : v. *supra* n°687.

[1729] C. pr. pén. art. R40-53.

[1730] V. *supra* n°691.

1029. Dans le cas du traitement de données informatiques captées[1731], une solution intermédiaire a été prévue avec une conservation des informations dans la base de données « jusqu'à la clôture des investigations » puis une mise sous scellés (mais traditionnels ici et non numériques) ensuite, assortie d'un effacement des données du traitement[1732].

1030. La neutralisation des contrôles potentiels par l'éparpillement des fichiers. – L'éparpillement des traitements judiciaires nuit à l'effectivité de leur contrôle lorsque celui-ci est prévu, puisque cela suppose de multiplier ceux-ci non seulement en termes de lieux à auditer, mais surtout de s'adapter aux différentes conditions d'accès et de mise en œuvre opérationnelle pour chacune de ces bases de données[1733]. Ainsi, dans le cas des données captées, comment est-on sûr que la mise sous scellés prévue s'accompagne bien de l'effacement des données en ligne ? On sait, par exemple, que dans le cas des écoutes téléphoniques, avant que la PNIJ ne soit mise en place, il était d'usage chez les enquêteurs qu'une copie soit mise sous scellés et versée à la procédure et qu'une autre copie soit conservée par les officiers de police judiciaire pour exploitation[1734].

Pourquoi n'en serait-il pas de même avec ces données qui sont censées être extraites du traitement ? Les données captées et celles gérées par la PNIJ, ne sont pas traitées de la même manière. La façon de procéder est encore différente avec les fichiers relatifs aux passé judiciaire d'une personne. Cette diversité neutralise l'efficacité des contrôles et confirme la vision des auteurs qui affirment que leur mise en œuvre reste souvent au stade de la théorie[1735].

1031. Conclusion de la section 1 : l'incohérence entre l'éparpillement et la protection des données personnelles. – L'éparpillement des traitements judiciaires est perçu comme protecteur pour les personnes fichées car il cloisonnerait les données collectées, évitant ainsi de créer une base de données où toutes les informations relatives

---

[1731] V. *supra* n°692.

[1732] Décret n°2015-1700 du 18 décembre 2015 relatif à la mise en œuvre de traitements de données informatiques captées en application de l'article 706-102-1 du code de procédure pénale, art. 5 : « Les données enregistrées sont conservées dans le traitement jusqu'à la date de clôture des investigations. A cette date, elles sont placées sous scellés fermés et effacées. »

[1733] GIQUEL François, *La CNIL exerce-t-elle un contrôle des fichiers de police suffisant ?*, Dalloz, AJ pénal 2007, p.69 : « si l'on compare la situation existante en 1978, date de création de la CNIL, à celle d'aujourd'hui, […] les fichiers se sont multipliés […]. »

[1734] Crim. 8 juillet 2015 n°15-81.731 : JurisData n°2015-016435. CHAVENT-LECLERE Anne-Sophie, *Les atteintes à la vie privée doivent répondre strictement aux garanties légales*, LexisNexis, Procédures n°10, octobre 2015, comm. 308.

[1735] V. *supra* n°1026.

à un individu seraient centralisées. Cette protection est illusoire car, au contraire, la dissémination neutralise et nuit à l'application des règles de protection des données personnelles. Les autorités judiciaires rechignent souvent à informer les personnes qu'elles font l'objet d'une saisie d'informations dans l'un des multiples fichiers accessibles en enquête pénale. L'éparpillement rend quasiment impossible à un individu d'exercer son droit d'accès qui lui permettrait de savoir si des données le concernant ont effectivement été collectées. De plus, la dissémination est associée à une multitude de régimes quant aux modalités de demandes d'effacement ou de rectification ce qui, une nouvelle fois, neutralise dans les faits les réelles possibilités que pourrait avoir une personne pour exercer ses droits. Cumulativement, du côté des autorités judiciaires, l'éparpillement complexifie les contrôles qui sont prévus puisqu'il est plus difficile de diligenter ces derniers au sein d'environnements différents.

1032. L'assimilation de l'éparpillement des traitements judiciaires avec la protection des données personnelles est donc incohérente, d'autant plus que, techniquement, la dissémination des données nuit également à la qualité des informations numériques collectées.

Section 2. L'incohérence entre l'éparpillement et la mise en œuvre technique des traitements judiciaires

1033. Les conséquences négatives de l'éparpillement des données sur la qualité et la fiabilité des informations conservées dans les traitements judiciaires. – La politique actuelle de l'Etat en matière de traitements judiciaires repose sur un éparpillement de ces fichiers auprès d'entités différentes. L'objectif est d'éviter un traitement rassemblant l'ensemble des informations personnelles recueillies par l'Etat au sujet d'une personne. Cette vision serait plus protectrice pour les individus fichés. Or, l'éparpillement des données, conséquence de la dissémination des traitements judiciaires, n'est pas cohérent avec les règles techniques prônées pour mettre en œuvre un système d'information contenant des données fiables et de qualité.

1034. Cette incohérence trouve l'une de ses sources dans la confusion qui existe entre l'éparpillement des données et la protection informatique des informations *(§1)*. Les conséquences techniques de l'éparpillement rendent incohérentes la gestion informatique des données contenues dans les traitements judiciaires lors de la mise en œuvre de ces derniers *(§2)*.

§1. La confusion entre éparpillement et protection informatique

1035. L'erreur de raisonnement. – Les données sont éparpillées auprès d'entités différentes, et donc dans des lieux différents. Le raisonnement qui voudrait que cet hébergement des données dans des lieux différents protège systématiquement les informations est techniquement erroné. En effet, au sein de la protection informatique d'un système d'information *(I)*, l'éloignement géographique des données n'est pas nécessairement un critère favorable *(II)*.

I – La protection informatique des données

1036. Le lien entre la technique et le cadre légal. – Les normes ISO 2700x[1736] relatives à la sécurité des systèmes d'information, mesurent celle-ci avec quatre critères : la disponibilité[1737], l'intégrité[1738], la confidentialité[1739] et l'auditabilité[1740] (ci-après DICA). Une loi de février 2018 donne une existence juridique[1741] au référentiel DICA. Dans le cas des traitements judiciaires, toutes les atteintes aux données pourraient avoir de lourdes conséquences pour les personnes fichées. En effet, en matière de données personnelles, le grand public se focalise sur des atteintes intentionnelles dont, tout particulièrement, le vol.

1037. Dans le référentiel DICA, ce dernier s'inscrit dans la violation de la confidentialité. Néanmoins, une atteinte à l'intégrité des données, quelle qu'en soit la cause[1742] pourrait avoir de très lourdes conséquences : la consultation d'un traitement pourrait extraire des données erronées ou, pire encore, celles d'un autre individu ayant de lourds antécédents judiciaires à la place d'une victime.

[1736] Norme ISO 27001, *Techniques de sécurité – Systèmes de gestion de la sécurité de l'information*, Afnor. Norme ISO 27002, *Techniques de sécurité – Code de bonne pratique pour la gestion de la sécurité de l'information*, Afnor.

[1737] Il faut pouvoir accéder au système.

[1738] L'intégrité se définit comme le fait d'entrer une valeur « A » dans le système, de la conserver, et d'extraire ultérieurement la même valeur « A ».

[1739] Seules les personnes ou les applications habilitées peuvent accéder au système.

[1740] Cette notion rejoint la preuve puisque le système doit permettre d'opposer des données (techniquement, cela est en lien étroit avec la traçabilité).

[1741] Loi n°2018-133 du 26 février 2018 portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité, article 1 : « La sécurité des réseaux et systèmes d'information consiste en leur capacité de résister, à un niveau de confiance donné, à des actions qui compromettent la disponibilité, l'authenticité, l'intégrité ou la confidentialité de données stockées […]. »

[1742] Intentionnelle avec un acte de malveillance ou involontaire (dysfonctionnement technique, erreur humaine).

1038. La distinction entre éparpillement et réplication. – Les normes ISO 2700x définissent, notamment, la notion de « plan de continuité de service ». Il s'agit de la capacité d'un système d'information à garantir un certain taux de disponibilité aux usagers. Lorsqu'une structure décide que ses informations numériques doivent être accessibles quasiment tout le temps[1743], le plan de continuité de service nécessite que les données soient répliquées[1744] en un autre lieu géographiquement distant[1745]. En cas de coupure de l'accès à l'infrastructure source, l'infrastructure cible prend le relai pour que les usagers puissent continuer à avoir accès aux données. Cette configuration, reposant sur plusieurs infrastructures informatiques redondantes, géographiquement distantes, ne doit pas être confondues avec l'éparpillement de l'hébergement des traitements judiciaires. En effet, l'ensemble de ces structures informatiques font partie d'un plan de continuité de service, et constitue donc un tout, destiné à héberger un système d'information.

1039. Un focus sur certaines règles techniques inhérentes à la protection des données permet de comprendre la confusion qui est faite en assimilant, à tort, l'éparpillement de l'hébergement des traitements judiciaires avec leur protection.

II – La confusion avec le critère de l'éparpillement

1040. La nécessité d'un raisonnement prenant en compte la dématérialisation. – La confusion provient d'un raisonnement élaboré sur des biens matériels, qui ne tient pas compte du contexte de la dématérialisation dont, notamment, l'immatérialité des données[1746]. En effet, la dématérialisation s'appuie sur des infrastructures informatiques complexes, composées de baies de serveurs et de stockages[1747]. L'accès aux informations est fortement tributaire des couches logicielles[1748]. Avec ce type d'environnement technique, il y a une dissociation entre le lieu physique où sont stockées les données et l'accès à ces dernières.

1041. Ainsi, pour reprendre l'exemple précédent, le cas du vol d'informations numériques n'est pas lié à l'accès à la salle blanche ou au *data center* dans lequel sont

[1743] Les taux les plus élevés dépassent les 99%.
[1744] La réplication consiste à copier les données en temps réel d'une infrastructure informatique source vers une infrastructure cible.
[1745] L'infrastructure cible doit être géographiquement distante car une coupure réseau d'une zone géographique importante pourrait isoler l'infrastructure source. En conséquence, pour être efficace, l'infrastructure cible doit être éloignée.
[1746] V. *supra* n°219.
[1747] Sur la notion de *Cloud*, v. *supra* n°221.
[1748] DAUERER Norman J. and KEKKEY Edward E., *Front end for file access controller*, Nov. 21, 1995.

enregistrées les informations relatives à un traitement judiciaire[1749]. Un individu qui pourrait accéder physiquement aux serveurs, se retrouverait, certes, devant des équipements informatiques contenant les données, mais aurait beaucoup plus de difficultés à voler les informations qu'une autre personne, située sur un site géographiquement distant, et ayant usurpé des codes d'accès informatiques[1750].

1042. L'éparpillement physique des traitements inopérant pour la protection du vol des informations numériques. – Face à ce risque que représente un accès frauduleux aux données[1751], le lieu de stockage physique des traitements judiciaires est sans importance. En premier lieu, plusieurs fichiers de police peuvent être stockés dans un même lieu mais être dotés d'accès différentiés[1752]. Inversement, ces mêmes traitements peuvent être hébergés dans des endroits géographiquement distants, mais les informations qu'ils contiennent peuvent être accessibles depuis une seule et même application[1753]. Ainsi, si l'accès permettant le vol est opéré par le biais de ce portail informatique, offrant l'accès à plusieurs traitements, l'hébergement en des lieux séparés est alors sans effet sur la protection des informations contenues. Pour l'individu procédant à l'accès frauduleux, les lieux de stockage sont sans importance.

En second lieu, en sécurité informatique, la majorité des fuites sont le fait de personnes dument habilitées qui, intentionnellement ou pas[1754] introduisent un code malveillant directement sur le réseau interne de leur lieu de travail[1755] ou, tout simplement, commettent une négligence. Par voie de conséquence, si cette personne, en raison de ses fonctions, a accès à différents traitements de données, la protection par leur éparpillement physique devient également inopérante.

[1749] Sur la dématérialisation du vol d'informations, v. JOUNIOT Sylvie, *Vol : avatars d'une infraction protéiforme*, Dalloz AJ pénal 2019 p.26.

[1750] V. par ex. le vol de données chez Uber, révélé en novembre 2017. Comme toujours dans ces vols de données personnelles, c'est par un accès dans le système d'information que les faits délictueux ont été commis. Dans le cas d'Uber, c'est par le biais d'un compte technique que les pirates ont pu, après plusieurs étapes, accéder aux données dérobées. Source : www.usine-digitale.fr

[1751] C. pén. art. 323-1 à 323-3.

[1752] Les accès peuvent ne pas être simplement différenciés par l'étape de l'identification, mais peuvent aller jusqu'à des accès réseaux physiques distincts.

[1753] V. par ex. ATHENA, dédié à la Gendarmerie, qui est appelé à devenir l'interface informatique des gendarmes pour leur fournir l'accès à l'ensemble des applications dont ils ont besoin.

[1754] Souvent, les personnes sont utilisées à leur insu pour, par exemple, introduire un code malveillant dans un système informatique, soit par un courriel qui leur est adressé soit au travers d'un support numérique qu'elles utilisent et qu'elles connectent sur leur poste de travail.

[1755] KAPFER Philippe, *Internal Hacking et contre-mesures en environnement Windows*, Editions ENI : « Si les entreprises redoublent d'efforts pour sécuriser leurs systèmes informatiques, des études montrent qu'elles se révèlent vulnérables de l'intérieur. »

1043. La sécurisation des données affaiblie par l'éparpillement physique des traitements judiciaires. – Néanmoins, l'accès physique à l'infrastructure de stockage n'est pas négligeable puisque le vol n'est pas le seul acte de malveillance susceptible de nuire aux données. Un accès physique frauduleux pourrait porter atteinte à l'intégrité et à la continuité des données[1756] selon le référentiel DICA. Ainsi, l'hébergement des traitements judiciaires doit être confié à des structures aptes à offrir un important degré de sécurité[1757]. Or, l'éparpillement des traitements judiciaires disperse inévitablement les moyens mis pour sécuriser une infrastructure informatique[1758]. Il est désormais possible de sécuriser une infrastructure informatique complète[1759] avec une fiabilité proche de 100%[1760]. Le pourcentage de fiabilité est surtout une affaire de moyens, ce qui prône un regroupement de l'hébergement dans un petit nombre de *data center*.

1044. Bien sûr, le « risque zéro » n'existe pas, mais le parallèle peut ici être fait avec une centrale nucléaire. Il n'est pas envisageable qu'une centrale nucléaire explose. Personne ne peut pourtant affirmer que c'est totalement impossible. En revanche, tout est fait pour que la probabilité soit la plus faible possible. La situation est comparable puisque la sécurisation quasi-parfaite d'une base de données unique est un objectif parfaitement définissable. D'ailleurs, le nouvel article 99 de la loi informatique et libertés[1761] va dans ce sens en énonçant, d'une part, l'obligation de procéder à une évaluation des risques pour les traitements prévus par l'article 87 de la même loi[1762] et, d'autre part, une liste précise de mesures techniques qui doivent être déployées pour protéger ces traitements.

[1756] Par ex, en détruisant physiquement l'infrastructure informatique, en arrachant des câbles réseaux, les données se seraient plus accessibles.

[1757] V. *infra* n°1112.

[1758] Cet éparpillement ne doit pas être confondu avec la réplication des données sur différentes infrastructures informatiques géographiquement distantes : v. *supra* n°1038.

[1759] Il faut ici dépasser la vision de la seule base de données hébergeant les informations, puisque dans une optique de sécurisation ce sont toutes les composantes techniques (réseaux, serveurs, logiciels, bases de données, etc), organisationnelles et juridiques (contrats de travail avec des obligations de confidentialité renforcées, contrat avec les tiers techniques, etc) qui contribuent à la sécurité globale du traitement de données à caractère personnel mis en œuvre.

[1760] LANDRY Pierre, *À la recherche de l'architecture de stockage absolue*, ITforBusiness, 1er octobre 2014 : « […] Infinidat cible les besoins de très haute disponibilité (99, 99999% soit 3 secondes d'arrêt par an...) avec une performance constante quelle que soit la charge ou les reconstructions de disque en cours. »

[1761] Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée par l'ordonnance n°2018-1125 du 12 décembre 2018 prise en application de l'article 32 de la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles et portant modification de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et diverses dispositions concernant la protection des données à caractère personnel.

[1762] Art 87 : « Le présent chapitre s'applique […] aux traitements de données à caractère personnel mis en œuvre, 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 […]. »

1045. Conclusion du paragraphe §1 : la confusion entre éparpillement et protection informatique. – La vision de données mieux protégées par la dissémination physique des traitements judiciaires est erronée. En premier lieu, cette vision trouve sa source dans une confusion qui applique un raisonnement valable pour les biens matériels, aux données. Or, l'immatérialité des informations numériques dans le contexte général de dématérialisation, fait que les risques principaux ne découlent pas des accès physiques à l'endroit où sont stockées les données, mais proviennent des accès informatiques qui sont réalisés à distance et qui sont totalement indépendants du lieu depuis lequel ils sont opérés. En second lieu, les règles de protection des systèmes d'information démontrent que la sécurisation des données nécessite d'important moyens, qui se traduisent évidemment par un coût financier. Dès lors, il est plus facile pour l'Etat de concentrer ses moyens pour sécuriser les données contenues dans les traitements judiciaires en limitant le nombre d'entités les hébergeant.

1046. D'ailleurs, l'éparpillement actuel des données se traduit par des incohérences dans la mise en œuvre technique.

§2. L'incohérence entre éparpillement et mise en œuvre technique

1047. L'incohérence avec des préconisations techniques. – L'éparpillement des données auprès d'entités va à l'encontre de règles techniques qui sont essentielles lors de la mise en œuvre d'un système d'information pour assurer la fiabilité et la qualité des informations numériques. D'une part, cet éparpillement ne permet pas de respecter l'une des règles informatiques les plus élémentaires en matière de fiabilité de l'information numérique, qui veut que la saisie multiple d'une même donnée soit éradiquée *(I)*.

Le non-respect de cette règle a pour conséquence une redondance importante de certaines informations d'un traitement judiciaire à un autre, sans qu'aucune synchronisation de ces informations ne soit prévue *(II)*.

I – Les effets négatifs de la saisie multiple d'une même donnée

1048. La saisie multiple d'une même donnée comme source d'information erronée. – Dans un système d'information, la fiabilité des données qui sont entrées dans le système impose de proscrire totalement la saisie multiple d'une même information.

Lorsqu'une donnée doit être entrée manuellement, même si elle est utilisée à de multiples reprises par la suite, elle ne doit être saisie qu'une seule fois[1763].

1049. En effet, plusieurs erreurs humaines[1764] sont identifiées lorsque des saisies multiples sont réalisées. Tout d'abord, la plus évidente est l'erreur de lecture ou de frappe lorsque la donnée est saisie par un opérateur. Ensuite, il peut s'agir d'une erreur dans la destination de la donnée[1765] et, enfin, l'erreur de déchiffrage qui est une variante de l'erreur de lecture mais à la différence que l'opérateur croit saisir la bonne donnée[1766]. L'ensemble de ces erreurs ont toutes pour conséquence de créer une nouvelle donnée illégitime, qu'il sera très difficile, voire impossible, postérieurement de corréler avec la bonne donnée et donc de corriger.

1050. Or, dans tous les traitements de données judiciaires, il existe un socle important de données communes[1767]. Outre l'identification[1768], on retrouve, à quelques variantes prés, le contexte de l'affaire ayant conduit à la collecte des données, ainsi que, souvent, les photos d'identification, et la qualification. Cette dernière, suivant le stade à laquelle est ouverte la fiche, peut simplement reposer sur les faits retenus par le parquet lors de l'enquête[1769], ou, au terme de la procédure, l'infraction pour laquelle un individu a été condamné de manière définitive[1770]. Ainsi, dans le contexte de l'éparpillement des traitements judiciaires, ce socle de données est précisément saisi plusieurs fois, par des opérateurs différents[1771]. Il y a là une première source majeure d'erreurs pour les informations contenues dans ces bases de données.

[1763] Ministère de la justice du Quebec, bureau de la sous-ministre et sous-procureure générale, *Plan directeur en ressources informationnelles du ministère*, 17 décembre 2019 : « Intégration inadéquate de l'information de justice : La désuétude des systèmes informatiques conduit à une difficile intégration de l'information entre les entités et les systèmes, ce qui oblige trop souvent la saisie multiple d'une même information. »

[1764] Sur l'importance des erreurs humaines dans le domaine de la sécurité informatique, v. DENIS Jérôme, *L'informatique et sa sécurité - Le souci de la fragilité technique*, Réseaux 2012/1 (n° 171), pages 161 à 187 : « […] l'informatique est décrite comme un univers où les mauvaises manipulations sont nombreuses, d'autant plus qu'elles peuvent rester invisibles aux yeux des utilisateurs lambda. »

[1765] La donnée est ici correctement saisie, mais pas au bon endroit dans le système. Dans le cas d'un traitement judiciaire, cela peut être, lors du changement d'adresse d'un individu fiché, l'opérateur qui ne modifie pas l'adresse dans le bon dossier.

[1766] Cette erreur sera fréquente lorsqu'un opérateur doit saisir des notes manuscrites.

[1767] V. *infra* n°1153.

[1768] Nom, prénom, adresse, téléphone. Souvent la profession.

[1769] Par ex., dans Cassiopée (v. *supra* n°990.). C. pr. pén. art. 48-1.

[1770] C'est le rôle du bulletin n°1 du Casier judiciaire (v. *supra* n°640.). C. pr. pén. art. 768 et 774.

[1771] Un greffier ou le secrétariat du Parquet dans le cas de Cassiopée, un agent du service du Casier judiciaire, un militaire ou un fonctionnaire de la Police dans le cas du TAJ.

1051. L'expérience du domaine de la santé pour éviter les conséquences d'une erreur due à de multiples saisies. – Pour comprendre l'importance de proscrire toute multiple saisie d'une même information, il est intéressant d'observer ce qui a été fait dans le domaine de la santé, où les données sont également fortement critiques. Ici, il a été identifié très tôt les erreurs qui ressortent de la saisie multiple d'une même information. C'est ainsi que le référentiel pour la certification des établissements de santé[1772] a imposé, dès 2010, l'informatisation du circuit du médicament pour éradiquer les erreurs imputables à de multiples re-saisies. Trop de problèmes dans l'administration des médicaments étaient, en effet, dues à une erreur de lecture et de saisie de l'ordonnance manuscrite du médecin, ou lors de la délivrance du médicament par la pharmacie interne de la structure hospitalière[1773], ou lors de la validation du plan de soins, ou enfin lors de l'administration du traitement par les infirmières. L'éventuelle détermination des responsabilités est, avec ce type d'erreur, d'une difficulté extrême[1774]. Les dossiers numériques de soins ou les dossiers patients informatisés ont, sur ce point, permis que le médecin prescrive directement sur un progiciel dédié[1775] et, toute la chaîne précédemment décrite étant la continuité de la saisie initiale du praticien, l'ensemble des erreurs qui viennent d'être exposées[1776] s'en sont trouvées naturellement éradiquées. Dans le cas des traitements de données judiciaires, une erreur de saisie peut également avoir de lourdes conséquences[1777].

1052. Le temps comme facteur aggravant. – Les données erronées contenues dans des fichiers de police dues à la saisie multiple ne peuvent que s'accentuer avec le temps, puisque dès qu'une mise à jour d'une information au sein du socle commun à plusieurs fichiers de police est nécessaire, les erreurs de saisies multiples sont à nouveau possibles. En effet, la donnée à actualiser nécessite autant de saisies que de traitements judiciaires dans lesquels elle est présente. En conséquence, au cours de la durée de vie, fort longue,

[1772] Il s'agit de la certification des établissements de santé (C. santé publique art. 6111-1 et s.) délivrée par la Haute Autorité de Santé (HAS). La HAS est définie aux art. L161-37 et s. du Code de la sécurité sociale. Dès la V2010 l'informatisation du circuit du médicament était demandée aux établissements de santé. Source : www.has-sante.fr

[1773] Certification des Logiciels d'Aide à la Dispensation (LAD) délivrée par la HAS. C. sécurité sociale art. L161-38.

[1774] VERNY Edouard, *La responsabilité pénale au sein de l'équipe médicale,* Dalloz, Revue de Droit Sanitaire et Social, 2008, p.58.

[1775] Certification des Logiciels d'Aide à la Prescription (LAP) délivrée par la HAS, *ibid.*

[1776] V. *supra* n°1049.

[1777] V. *supra* n°1015.

des données contenues dans les traitements judiciaires, les erreurs dues à la redondance des informations deviennent exponentielles.

1053. On comprend alors notamment, comment des situations ubuesques où les forces de police interviennent dans un appartement qui n'est plus occupé par les individus, cibles de l'intervention, peuvent se produire, notamment en raison d'un défaut de mise à jour de l'adresse d'individus fichés[1778].

1054. La saisie multiple en corrélation directe avec l'éparpillement des traitements. – Les traitements judiciaires sont composés d'un socle important d'informations communes[1779]. Cette redondance a pour effet que les fiches ne sont pas gérées et mises à jour dans une même base, mais au contraire par des opérateurs différents qui re-saisissent plusieurs fois la même information. Il y a là une source importante d'erreurs qui se cumule avec le fait que les données communes dans différents traitements judiciaires ne bénéficient d'aucune synchronisation technique.

II – <u>Les effets négatifs de la non-synchronisation des données</u>

1055. La nécessité d'avoir une base de données de référence. – Si l'on dépasse le seul cadre des traitements judiciaires, « l'idéal informatique » est de regrouper toutes les données dans une base unique[1780]. Toutefois, ceci n'est pas toujours possible. Il existe un grand nombre de raisons pour que des bases de données soient distinctes et séparées. La plus courante provient simplement de l'historique de construction d'un système d'information[1781]. Dans un atelier de production, par exemple, il est rarissime que toutes les machines aient été achetées au même fournisseur. De même, tous les logiciels composant un système d'information ne sont pas installés au même moment ou bien un même éditeur ne développe pas des solutions répondant à la transversalité des besoins de ses clients. En conséquence, il est classique que des bases de données distinctes contiennent des informations redondantes. Toutefois, la règle informatique veut qu'il y ait une source qui fasse foi et que les autres bases de données viennent lire les

[1778] 20 Minutes, *Nice : Le Raid se trompe d'appartement et blesse une fillette*, 19 novembre 2015.
Le Parisien, *Perquisition à Clichy-sous-Bois : « Madame, désolé, on s'est trompé »*, 29 novembre 2015.
[1779] V. *infra* n°1153.
[1780] Ce que l'on nomme en langage informatique : « consolider » des bases de données.
[1781] PARISOT Thierry, *L'organisation mise en place aux achats sert de modèle à la DSI*, ITforBusiness, 1er mars 2015, entretien avec Charles-Henri VOLLET, Directeur des achats et des systèmes d'information groupe, Mersen : « Du fait de l'historique […], il y avait une très grande hétérogénéité : 25 ERP, 7 opérateurs télécoms et 4 technologies pour le réseau mondial de transfert de données, 22 messageries, un parc micro composé de toutes les marques qui existaient à l'époque... »

informations dont elles ont besoin dans cette base source, ceci dans l'objectif évident d'éviter à devoir re-saisir manuellement ces informations déjà numérisées[1782].

1056. Ce mécanisme se nomme l'interopérabilité[1783]. Il constitue l'une des composantes essentielles de l'intégration des différents logiciels dans un système d'information existant[1784]. Si l'on reprend l'exemple des systèmes d'information de santé, la base qui fait foi est souvent le logiciel administratif qui gère l'admission des patients, avec la saisie de leurs données d'identification, de leur identifiant de santé[1785], et qui attribue un numéro unique de séjour au patient. Les logiciels qui concourent au suivi médical des patients[1786] viennent alors s'interfacer avec le logiciel administratif afin d'y récupérer les données dont ils ont besoin pour fonctionner. Aucune re-saisie des données composant le socle commun n'est évidemment réalisée manuellement.

1057. Les prémices de l'interopérabilité en matière de traitements judiciaires. – Dans le cas des traitements judiciaires, les pouvoirs publics envisagent de faire jouer un rôle similaire à Cassiopée, qui tendrait à devenir la référence imposant les mises à jour aux autres traitements[1787]. Toutefois, la situation reste compliquée et l'interopérabilité en est encore au « stade expérimental[1788] ». Il est indéniable que Cassiopée a un véritable rôle à jouer pour imposer aux autres traitements de données judiciaires les mises à jour relatives à la qualification des faits, aux classements sans suite, aux non lieux, aux relaxes ou aux acquittements puisque Cassiopée a la légitimité parfaite pour tenir ce rôle. En effet, ce logiciel est sous le contrôle des magistrats[1789].

1058. Néanmoins, pour toutes les autres données, il faut envisager que la mise à jour des informations puisse provenir de n'importe quel traitement qui, pour une raison ou une

---

[1782] V. *supra* n°1048.
[1783] V. *infra* n°1206.
[1784] Sur la nécessité que les différentes composantes du système d'information échangent des informations, v. VARANDAT Marie, *Actia optimise ses process à l'échelle internationale avec un PLM*, ITforBusiness, 16 mars 2018 : « Cette croissance externe a entraîné une grande hétérogénéité au niveau des systèmes d'information avec des applications qui ne communiquaient pas et des process variés qui freinaient la collaboration au sein des équipes. »
[1785] Code de la santé publique, art. L1111-8-1.
[1786] Dossier Patient Informatisé, logiciels spécifiques à des activités telles que l'anesthésie, le bloc opératoire, etc.
[1787] V. *supra* n°625.
[1788] BEYNEL Jean-François et CASAS Didier, *Chantiers de la justice – Transformation numérique*, Ministère dela Justice, 2018 : « Mise à disposition de nombreuses applications expérimentales (les échanges inter-applicatifs entre le Casier Judiciaire et Cassiopée […]. »
[1789] C. pr. pén. art. R15-33-66-4 : « Ce traitement a pour objet l'enregistrement d'informations et de données à caractère personnel relatives aux procédures judiciaires au sein des tribunaux judiciaires, afin de faciliter la gestion et le suivi de ces procédures par les magistrats, les greffiers et les personnes habilitées qui en ont la charge […]. »

autre, prend en compte, par exemple, le changement de domicile d'un individu. Dans le cas, notamment, des personnes faisant l'objet d'une inscription dans le fichier judiciaire national automatisé des auteurs d'infractions sexuelles ou violentes ou encore celui des auteurs d'infractions terroristes, il leur est demandé de signaler tout changement d'adresse[1790]. Ainsi, pour des informations telles que la domiciliation, Cassiopée n'est pas forcément la référence qui doit s'imposer aux autres fichiers.

1059. Une ambiguïté malheureuse avec le traitement d'antécédents judiciaires. – Alors que le TAJ est un fichier de police d'une forte criticité en raison du volume de données qu'il contient et de sa facilité d'accès pour les enquêteurs de terrain[1791], une ambiguïté ressort de l'article 230-8 du Code de procédure pénale. Ce dernier, dans son deuxième alinéa, semble imposer les décisions du procureur de la République en matière d'effacement ou de rectification des informations aux autres traitements[1792].

1060. En premier lieu, cet asservissement des autres fichiers judiciaires aux décisions du procureur soulève la question de la partialité. Le procureur représente les intérêts de la société et a en charge la mise en œuvre de la politique pénale décidée par le Parlement[1793]. Avec Cassiopée, comme précédemment expliqué[1794], ce sont les décisions des juges du fond qui sont susceptibles d'être répercutées dans les autres traitements ce qui, *a contrario*, est légitime. En second lieu, d'un point de vue technique, cette disposition de l'article 230-8 vient à l'encontre des efforts d'interopérabilité initiés avec Cassiopée puisqu'il est clairement sous-entendu que les décisions du procureur de la République « sont portées à la connaissance des responsables de tous les traitements automatisés » par le biais d'une communication classique et, en aucun cas, au travers

[1790] Pour le fichier judiciaire national automatisé des auteurs d'infractions sexuelles ou violentes, v. C. pr. pén. art. 706-53-5.
Pour le fichier judiciaire national automatisé des auteurs d'infractions terroristes, v. C. pr. pén. art. 706-25-7.
V. *supra* n°994.
[1791] V. *supra* n°995.
[1792] C. pr. pén. art. 230-8 : « […] Les décisions d'effacement ou de rectification des informations nominatives prises par le procureur de la République sont portées à la connaissance des responsables de tous les traitements automatisés pour lesquels, sous réserve des règles d'effacement ou de rectification qui leur sont propres, ces mesures ont des conséquences sur la durée de conservation des données à caractère personnel. […] »
[1793] VOLFF Jean, *Elaborer et mener la politique pénale d'un parquet*, Recueil Dalloz 2009 p.317.
[1794] V. *supra* n°1057.

d'une mise à jour automatique ou semi-automatique[1795] qui éviterait des erreurs de saisies[1796].

1061. Une mauvaise utilisation du TAJ pour les mises à jour. – Outre les décisions d'effacement et de rectification des informations en cas de requalification judiciaire[1797], de mise hors de cause de la personne concernée, d'effacement du bulletin n°2 du casier judiciaire, le TAJ devrait pouvoir jouer un rôle dans la mise à jour de toutes les informations relatives aux coordonnées et la domiciliation d'un individu. En effet, ce logiciel étant au plus près des enquêteurs, il est nécessairement celui dont les informations de proximité ont le plus de chance d'être actualisées et il serait alors essentiel d'en profiter pour mettre à jour les autres fichiers de police afin d'éviter, notamment, des perquisitions à de mauvais endroits[1798]. Pour de telles informations, l'interopérabilité entre les différents traitements pourrait jouer un rôle important.

1062. Conclusion du paragraphe §2 : l'incohérence entre éparpillement et mise en œuvre technique. – Le cloisonnement total des données qui résulte de l'éparpillement des traitements judiciaires est en contradiction avec des règles techniques élémentaires de gestion des informations numériques. Alors que toute re-saisie ou saisie multiple d'une même donnée est à proscrire absolument[1799], l'éparpillement des traitements judiciaires a pour effet de conduire des intervenants à enregistrer, manuellement et à maintes reprises, des informations communes à un ou plusieurs fichiers. Cette saisie multiple est, d'une part, une source d'erreur importante et, d'autre part, nuit évidemment à la mise à jour de ces informations communes car il est impossible, en l'état actuel, de propager efficacement l'évolution d'une donnée dans l'ensemble des traitements judiciaires où elle est commune.

1063. Conclusion du chapitre 1 : la protection illusoire des personnes fichées par l'éparpillement des données. – Contrairement à une idée qui provient des prémices des traitements mis en œuvre par l'Etat, à une époque où ils étaient peu nombreux et où ils

[1795] V. *infra* n°1207.
[1796] V. *supra* n°1049.
[1797] Sur les effets de la requalification judiciaire sur le TAJ, v. notamment BUISSON Jacques, *Preuve – Moyens de la preuve*, Dalloz Répertoire de droit pénal et de procédure pénale, Octobre 2019, chapitre 1, al.72.
[1798] V. *supra* n°1053.
[1799] V. *supra* n°1049.

avaient une finalité claire et unique, l'éparpillement physique des traitements judiciaires nuit fortement aux droits des personnes fichées. En effet, les besoins croissants des autorités judiciaires de collecter et de conserver des données indispensables à l'efficacité des enquêtes pénales génèrent une augmentation exponentielle du nombre de traitements judiciaires[1800]. Or, face à une telle multiplication, l'éparpillement de ces fichiers et le cloisonnement des données qui en découle, ne sont plus cohérents avec l'idée initiale de protection des personnes fichées. En premier lieu, cet éparpillement est un obstacle à l'application des obligations qui incombent à un responsable de traitement dans le cadre de la protection des données personnelles. En second lieu, le cloisonnement physique des données qui découle de la dissémination des fichiers nuit, pour des raisons techniques, à la qualité et la fiabilité des informations enregistrées, ce qui, inévitablement, peut nuire aux personnes fichées.

1064. Il est donc nécessaire de dépasser la vision faussement protectrice de l'éparpillement des traitements judiciaires pour étudier la possibilité de concilier le maintien de la séparation des traitements aux finalités différentes, avec le regroupement de certaines données communes à plusieurs de ces fichiers.

[1800] V. *supra* n°973.
VEDEL Renaud, *Le rôle des fichiers dans l'action opérationnelle des services de sécurité intérieure*, Dalloz AJ pénal 2007 p.64 : « Une police sans documentation par fichier serait entravée car sans mémoire, sans capacité d'investigation à un coût supportable, sans moyen de preuve. »

Chapitre 2. La cohérence des traitements judiciaires améliorée par le regroupement des données

1065. La nécessité de regrouper certaines données des traitements judiciaires. – L'extraction de données depuis les traitements judiciaires[1801] constitue la deuxième catégorie d'investigations numériques[1802]. Le principe de l'éparpillement physique des données dû à la dissémination des traitements judiciaires au sein d'entités différentes, présente des défauts importants, dont les conséquences sont néfastes pour les libertés individuelles et pour l'efficacité de l'enquête[1803]. La possibilité de regrouper certaines données des traitements judiciaires constitue un enjeu majeur pour améliorer la qualité et le contrôle des informations numériques composant les traitements judiciaires. Bien sûr, l'existence d'un fichier unique et centralisé regroupant toutes les données n'est pas envisageable. Tout d'abord, parce que les enquêteurs ont accès à des traitements purement administratifs[1804] comme le fichier des cartes grises ou des permis de conduire[1805]. Ensuite, car d'autres fichiers viennent en support de la mission de police administrative de la Gendarmerie et de la Police nationales et s'inscrivent donc dans une logique de préservation de l'ordre public[1806]. Ces traitements ne sont pas donc pas placés sous la responsabilité des autorités judiciaires[1807].

1066. La nécessité d'un changement sans bouleversement. – Un tel changement de paradigme ne doit pas chambouler l'ensemble du cadre légal et règlementaire des traitements judiciaires, composé aussi bien de dispositions codifiées dans le Code de

[1801] V. *supra* n°968.
[1802] V. *supra* n°603.
[1803] V. *supra* n°967.
[1804] GRANGER Marc-Antoine, *La distinction police administrative / police judiciaire au sein de la jurisprudence constitutionnelle*, Dalloz RSC 2011 p.789.
[1805] V. *supra* n°698.
[1806] Par ex. l'EASP et le PASP : v. *supra* n°709.
[1807] V. *supra* n°696.

procédure pénale[1808] ou de la sécurité intérieure[1809], que de décrets ou d'arrêtés[1810], encadrant l'ensemble des traitements existants actuellement. L'objectif est de faire converger les possibilités techniques qu'offre l'informatique et les grands principes juridiques qui entourent les données à caractère personnel.

1067. L'étude d'une consolidation mesurée des données judiciaires. – Dans un premier temps, il est nécessaire d'étudier la possibilité de créer une entité permettant la mise en commun crédible et réaliste de certaines données judiciaires directement accessibles en enquête pénale *(Section 1)*. L'entité destinée à regrouper ces données serait appelée la « Base Nationale des Données Judiciaires[1811] (ci-après BNDJ) ». Dans un second temps, l'étude du régime de cette BNDJ doit, notamment, décrire avec précision les règles qui s'appliqueraient aux données des traitements judiciaires qui bénéficieraient de cette entité. *(Section 2)*.

Section 1. La proposition du regroupement des données par la création de la BNDJ

1068. L'étude de la création d'une entité pour regrouper les données. – La consolidation de certaines données contenues jusqu'à présent dans différents traitements judiciaires pourrait renforcer l'équilibre entre l'efficacité des investigations numériques d'extraction de données, et la protection des libertés individuelles[1812]. Pour parvenir à cette consolidation, la présente étude propose la création d'une entité permettant de regrouper et de lier certaines données présentes dans les différents traitements judiciaires.

1069. Pour créer une telle entité, il est nécessaire de distinguer l'étude de sa création proprement dite *(§1)*, de l'étude des règles générales qui autoriseraient le regroupement de certaines données au sein de cette nouvelle entité *(§2)*.

[1808] V. *supra* n°961.

[1809] V. par ex. C. sec. int. Livre I[er], Titre III, Chapitre II : « Traitements automatisés de données recueillies à l'occasion de déplacements internationaux » - V. *supra* n°704.
C. sec. int. Livre I[er], Titre III, Chapitre III : « Contrôle automatisé des données signalétiques des véhicules » - V. *supra* n°682.
C. sec. int. art. R236-1 et s. : « Enquêtes administratives liées à la sécurité publique » (EASP) – v. *supra* n°709.
C. sec. int. art. R236-11 et s. : « Prévention des atteintes à la sécurité publique » (PASP) – *Ibid.*

[1810] V. *supra* n°961.

[1811] V. *infra* n°1071.

[1812] V. *infra* n°1106.

§1. L'étude de la création de la BNDJ

1070. Les bases de l'étude de la création d'une BNDJ. – En premier lieu, le nom de l'entité permettant de regrouper et de lier certaines données présentes dans des traitements de données judiciaires physiquement séparés doit faire l'objet d'une attention particulière car il doit incarner la transparence et la clarté de la finalité cette entité *(I)*. En second lieu, la démarche législative et règlementaire qui serait nécessaire pour créer une telle entité doit être présentée *(II)*.

I – La cohérence de la dénomination

1071. La rigueur dans le choix des mots. – L'intitulé des traitements de données judiciaires soulève parfois des difficultés, lorsque le nom ne correspond pas aux informations qui y sont collectées[1813]. La dénomination de l'entité informatique qui serait appelée à regrouper plusieurs fichiers de police actuels doit donc faire l'objet d'un choix rigoureux. Il y aurait là un impératif de transparence et de cohérence[1814].

1072. L'entité appelée à héberger les données. – Tout d'abord, le mot « traitement » ne doit pas être utilisé. En effet, le RGPD[1815] défini celui-ci comme désignant des actions informatiques qui sont réalisées sur des données[1816]. Le « traitement » est donc l'opération informatique qui correspond aux finalités énoncées pour les traitements judiciaires existants. Or, l'objectif de l'entité étudiée ici, n'est pas de regrouper les traitements au sens du RGPD, mais de mettre en commun certaines données identiques présentes au sein de ces différents traitements actuels. Le cloisonnement des traitements eux-mêmes peut être maintenu malgré une mise en commun informatique des données[1817]. Ainsi, cette entité informatique doit être désignée par un mot plus général

[1813] V. *supra* n°978.
[1814] NABAT Yoann, *Traitement automatisé de données personnelles - Lorsque la Cour européenne des droits de l'homme s'intéresse au fichage des manifestants... échos lointains de débats français*, LexisNexis Droit pénal n° 6, Juin 2019, comm. 116 : « Le vocabulaire est en droit si fondamental qu'il ne peut se satisfaire de ces mots à géométrie variable et d'une « terminologie trop imprécise » […]. »
[1815] 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).
[1816] RGPD, *Op cit.* p.12. art. 4 : « 2) « traitement », 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. »
[1817] V. *infra* n°1090.

que celui de « traitement » puisque celle-ci est précisément appelée à héberger plusieurs traitements[1818].

1073. Ensuite, le mot « fichier » ne sera également pas retenu. Le RGPD[1819] introduit une forte dichotomie entre la définition qu'il en donne et la définition informatique de ce mot[1820]. Informatiquement, un fichier est une entité regroupant des données que l'on peut qualifier d'élémentaire. En effet, le moindre traitement de données repose, informatiquement, sur un nombre très important de fichiers, et non sur un seul comme semble le suggérer le RGPD. De plus, le mot « fichier » est souvent utilisé par les autorités publiques comme synonyme de « traitement » en matière de traitements de donnés judiciaires[1821].

1074. Enfin, c'est la notion de « base de données » qu'il est préférable de retenir car c'est celle qui correspond le mieux à la définition de « fichier » explicitée par le RGPD. Certes, elle fait partie du vocabulaire technique, mais elle a l'avantage de rester générique, en portant la connotation d'un stockage de données, sans faire obstacle au fait que plusieurs traitements de données sont mis en œuvre en son sein. La notion de « base de données » concrétise donc la nécessaire distinction entre les traitements judiciaires et les données qui y sont enregistrées.

1075. La constance du mot « nationale ». – Le mot « nationale » doit qualifier cette base de données par homogénéité et continuité avec plusieurs traitements judiciaires actuels[1822] aux rôles majeurs.

[1818] *Ibid*.

[1819] *Op cit.* p.12. art. 4 : « 6) « fichier », 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. »

[1820] Fichier : « ensemble organisé d'informations, désigné par un nom précis, que le système d'exploitation d'un ordinateur manipule comme une simple entité, dans sa mémoire ou sur un support de stockage. » *Source : Larousse.*

[1821] V. *supra* n°826.
V. également le « fichier des personnes recherchées » (v. *supra* n°655.), le « fichier automatisé des empreintes digitales » (v. *supra* n°661.), le « fichier national automatisé des empreintes génétiques » *(ibid.)*, le « fichier judiciaire national automatisé des auteurs d'infractions sexuelles ou violentes » (v. *supra* n°667.), le « fichier judiciaire national automatisé des auteurs d'infractions terroristes » *(ibid.)*, le « fichier des objets et des véhicules signalés (FOVeS) » (v. *supra* n°684.) et les « Fichiers d'analyse sérielle » (v. *supra* n°720.).

[1822] « Fichier national automatisé des empreintes génétiques », « fichier judiciaire national automatisé des auteurs d'infractions sexuelles ou violentes », « fichier judiciaire national automatisé des auteurs d'infractions terroristes », « plate-forme nationale des interceptions judiciaires (PNIJ) ».

1076. La finalité judiciaire de la base de données. – Le mot « judicaire » qualifie les données destinées à être enregistrées. On pourrait, comme pour le mot « nationale », justifier l'emploi de celui-ci pour assurer la cohérence les fichiers actuels. Toutefois, il existe ici une raison plus importante. Le mot « judiciaire » est ce qui se réfère au juge[1823]. Or, le juge doit être l'ordonnateur des données saisies ou, à tout le moins, celui qui décide si elles doivent y être maintenues[1824]. L'autre lien inextricable avec le juge, est la qualification des faits qui doit subsister dans les traitements de données. Sur ce point, on relèvera que le traitement d'antécédents judicaires comporte le mot « judiciaire » de manière assez inopportune car il s'agit du fichier de travail des officiers de police judiciaire au quotidien et les données qui y sont enregistrées sont, dans les faits, très éloignées des décisions prises par les juges[1825]. Le fait de confier au juge la mise à jour de la qualification inscrite dans les traitements judiciaires constituerait une évolution favorable pour le respect des droits des personnes fichées, en supprimant « la distinction entre mémoire judiciaire et mémoire policière[1826] ».

1077. La Base Nationale de Données Judiciaires (ci-après BNDJ). – L'entité appelée à regrouper certaines données, actuellement physiquement séparées, présentes dans des traitements judiciaires différents, pourrait être désignée sous le nom de BNDJ. La distinction entre l'hébergement des données regroupées et les traitements eux-mêmes serait explicitée au travers de cette dénomination, et son placement sous le contrôle du juge serait affirmé.

[1823] CORNU Gérard, *Vocabulaire juridique,* 10ème édition, puf : « qui émane d'un juge ».
CADIET Loïc et JEULAND Emmanuel, *Droit judiciaire privé,* LexisNexis, p. 2 : « L'instrument de cette solution est le juge » [au sujet de l'objet du droit judiciaire].
[1824] BEGRANGER Gérald, *Le contrôle des fichiers de police par les juges*, Dalloz AJ pénal 2014 p.176.
[1825] V. *supra* n°1060.
[1826] GRUNVALD Sylvie, *Casier judiciaire et effacement des sanctions : quelle mémoire pour la justice pénale ,?* Dalloz AJ pénal 2007 p.416 : « […]la proposition de l'amélioration de l'information des personnes mises en cause dans les fichiers de police judiciaire sur l'existence de leurs droits d'accès et de rectification est actuellement écartée. Cette dernière position peut étonner en particulier lorsqu'elle a pour conséquence de ne pas admettre comme essentielle "que la qualification judiciaire des faits soit substituée à la qualification initiale telle qu'elle est enregistrée dans ces fichiers". La distinction entre mémoire judiciaire et mémoire policière est entérinée. »

II – La démarche pour la création

1078. La démarche légale et règlementaire. – Après avoir donné un nom cohérent à l'entité, dont l'objectif serait de regrouper et de lier certaines données actuellement présentes dans des traitements judiciaires physiquement séparés, la méthode pour lui donner une existence légale doit être précisée.

1079. Une proposition de loi. – De nombreuses dispositions relatives aux traitements judiciaires actuels sont issues de textes législatifs[1827] et ne peuvent donc être modifiées que par la Loi. Or, la « proposition de loi visant à améliorer l'efficacité et à renforcer les garanties des traitements de données en procédure pénale », précédemment décrite[1828], pourrait comporter ces modifications, en intégrant un second chapitre intitulé « dispositions relatives à la base nationale des données judiciaires ». Cette proposition de loi fait l'objet de l'annexe 2.

1080. Un projet de décret d'application. – La proposition de loi visant à créer la BNDJ est un texte portant des dispositions générales et structurantes pour la procédure pénale. Elle doit être complétée par un projet de décret d'application dont l'objectif serait de préciser les dispositions générales créées par la loi[1829]. Ce projet de décret, intitulé « projet de décret pris en application des dispositions relatives à la base nationale des données judiciaires » fait l'objet de l'annexe 4. Bien évidemment, la création de la BNDJ imposerait également de modifier certaines règles règlementaires relatives aux traitements judiciaires actuels afin d'autoriser le regroupement ou les corrélations d'informations numériques que ces derniers comportent.

1081. Le projet de « décret pris en application des dispositions relatives à la base nationale des données judiciaires » comporterait également ces modifications qui découlent directement de la création de la BNDJ, et qui concerneraient des dispositions éparpillées dans de nombreuses parties du Code[1830] voire dans certains textes restés non codifiés[1831].

[1827] Ex. : les fichiers d'analyse sérielle, le fichier national automatisé des empreintes génétiques, le fichier national automatisé des auteurs d'infractions sexuelles ou violentes, etc.

[1828] V. *supra* n°824.

[1829] V. annexe 2, proposition de loi, article 10, nouvel art. 230-53 : « Un décret en Conseil d'Etat, pris après avis de la Commission nationale de l'informatique et des libertés, fixe les modalités d'application du présent chapitre. […] »

[1830] V. *supra* n°630.

[1831] V. le fichier automatisé des empreintes digitales prévu par le décret n°87-249 du 8 avril 1987 relatif au fichier automatisé des empreintes digitales géré par le ministère de l'intérieur. Le seul lien entre le Code de procédure pénale et ce texte se fait au travers de l'art. R40-38-1 qui dispose que « le fichier automatisé des empreintes digitales est régi par le décret n°87-249 du 8 avril 1987 modifié relatif au fichier automatisé des empreintes digitales géré par le ministère de l'intérieur ».

1082. L'avis préalable de la CNIL. – Ces deux textes devraient être soumis à l'avis préalable de la CNIL avant de pouvoir être votés ou publiés[1832]. Une analyse d'impact prévue par la loi informatique et libertés issue des différentes modifications découlant de l'entrée en vigueur du RGPD ne serait pas nécessaire, car la BNDJ n'aurait pas pour conséquence de supprimer le cloisonnement des données sensibles contenues dans des traitements différents. En revanche, comme le prévoit la deuxième partie de l'article 90 de cette loi[1833], la CNIL devrait effectivement être consultée préalablement puisque la BNDJ introduirait de « nouveaux mécanismes, technologies ou procédures » pour traiter les informations enregistrées.

1083. La description des dispositions des deux projets de texte. – L'ensemble des dispositions nécessaires à la création et au fonctionnement de la BNDJ qui sont décrites et étudiées dans la suite des présentes sont réparties au sein de ces deux projets de textes, placés en annexe 2 et 4 des présentes.

1084. Conclusion du paragraphe §1 : l'étude de la création de la BNDJ. – La proposition de créer une entité permettant de regrouper des données présentes dans différents traitements judiciaires nécessite trois étapes. La première, qui vient d'être réalisée, consiste à indiquer un socle cohérent pour créer cette entité, en lui donnant un nom reflétant sa finalité judiciaire, et en décrivant les démarches légales et règlementaires qui seraient nécessaires pour sa création. Une deuxième étape consiste à définir les règles générales permettant d'identifier les données susceptibles d'être regroupées de celles qui devraient rester séparées.

[1832] Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée par l'ordonnance n°2018-1125 du 12 décembre 2018 prise en application de l'article 32 de la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles et portant modification de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et diverses dispositions concernant la protection des données à caractère personnel, art.89 : « Si le traitement est mis en œuvre pour le compte de l'Etat pour au moins l'une des finalités énoncées au premier alinéa de l'article 87, il est prévu par une disposition législative ou réglementaire prise dans les conditions prévues au I de l'article 31 et aux articles 33 à 36.
II.- Si le traitement porte sur des données mentionnées au I de l'article 6, il est prévu par une disposition législative ou réglementaire prise dans les conditions prévues au II de l'article 31. »

[1833] *Ibid.* art.90 : « […] Dans les autres cas, le responsable de traitement ou son sous-traitant consulte la Commission nationale de l'informatique et des libertés préalablement à la mise en œuvre du traitement de données à caractère personnel, qui se prononce également dans les délais prévus à l'article 34 : […] « 2° Soit lorsque le type de traitement, en particulier en raison de l'utilisation de nouveaux mécanismes, technologies ou procédures, présente des risques élevés pour les libertés et les droits des personnes concernées. »

§2. L'étude du regroupement des données dans la BNDJ

1085. Une entité informatique associant mise en commun et séparation. – La création de la Base Nationale de Données Judiciaires a pour objectif de permettre le regroupement et le lien entre certaines données actuellement présentes dans différents traitements judiciaires. En aucun cas la BNDJ n'a vocation à créer un gigantesque fichier de police au sein duquel toutes les informations contenues dans les actuels traitements de données judiciaires seraient regroupées sans distinction. Au contraire, elle doit permettre la mise en commun de certaines données telles que celles relatives à la domiciliation et aux coordonnées[1834], afin d'améliorer la fiabilité de ces informations dans l'ensemble des traitements, mais doit maintenir un cloisonnement des données sensibles[1835]. Cet équilibre doit être défini *(I)*. Le regroupement de plusieurs fichiers de police dans une même entité informatique permettrait de faciliter et de renforcer les contrôles de ces traitements *(II)*.

I – L'équilibre entre mise en commun et étanchéité des données

1086. La création de la BNDJ sans déstabilisation de la procédure pénale. – Les effets de la numérisation de notre société[1836] ne doivent pas imposer un bouleversement complet des investigations en procédure pénale[1837]. Certes, leurs spécificités doivent être prises en compte afin d'améliorer, aussi bien l'efficacité de l'enquête que le respect des libertés individuelles, comme en créant la BNDJ, mais l'adaptation à ces spécificités ne doit pas engendrer une instabilité juridique en introduisant un énième régime dérogatoire à la procédure pénale de droit commun[1838]. En conséquence, la BNDJ doit apporter des améliorations sans remettre en question tous les principes en vertu desquels sont créés les traitements de données judiciaires depuis que la dématérialisation des fichiers de police a commencé.

1087. La BNDJ n'est pas un fichier de police supplémentaire. – C'est pourquoi l'objectif de la BNDJ n'est pas de constituer un nouveau fichier de police mais de créer

---

[1834] V. *supra* n°1050.

[1835] Les informations contenues dans le « fichier national automatisé des empreintes génétiques », le « fichier judiciaire national automatisé des auteurs d'infractions sexuelles ou violentes », le « fichier judiciaire national automatisé des auteurs d'infractions terroristes », etc, ne doivent rester accessibles que pour des consultations strictement encadrées et définies.

[1836] V. *supra* n°17.

[1837] V. *supra* n°53.

[1838] Sur l'instabilité de la procédure pénale due aux multiples régimes dérogatoires introduits par les successions de loi, v. De LAMY Bertrand, *Procédure pénale - La constitutionnalisation de la procédure pénale*, LexisNexis Droit pénal n° 4, Avril 2019, dossier 3.

une entité informatique, sous la forme d'une base de données, destinée à héberger un ensemble de traitements judiciaires accessibles au stade de l'enquête. Cet hébergement mutualisé qui est, techniquement, parfaitement compatible avec le fait que les traitements restent séparés, a pour unique objectif de permettre le regroupement pertinent de certaines données enregistrées dans des fichiers différents.

1088. Un nouveau traitement de données dédié au contrôle des accès. – Néanmoins, la BNDJ créerait un nouveau traitement dédié à la gestion des droits d'accès[1839] et, surtout, à la traçabilité de ces accès[1840] ainsi que de toutes les opérations réalisées sur les données judiciaires, sans qu'aucune nouvelle information relative aux justiciables ne soit introduite. A ce titre, la BNDJ doit toutefois respecter les règles de la loi informatique et libertés[1841]. Ce premier rôle de la BNDJ, présenté à l'illustration n°4 (voir page suivante), constitue une amélioration importante s'inscrivant dans le respect des nouvelles dispositions issues de la mise en conformité de la loi informatique et libertés avec l'entrée en vigueur du RGPD[1842] et de la directive relative aux traitements de données judiciaires[1843] qui impose une « journalisation[1844] ».

[1839] Il s'agit des droits d'accès au sens informatique, à savoir le paramétrage des utilisateurs qui sont autorisés à se connecter à la BNDJ et à quelles informations ils ont accès. V. *infra* n°1123.

[1840] Sur la nécessité de conserver d'identifier la personne ayant consulté un fichier de police et donc de mettre en œuvre la traçabilité adéquate, v. crim. 19 février 2019 n°18-84.671, bull. crim. 2019 n°38, Obs. D. 2019 p.434 : « […] les motifs sont insuffisants à établir que l'accès au fichier LAPI [v. *supra* n°682.] a été le fait soit d'un agent régulièrement habilité […] soit d'un enquêteur autorisé par le procureur de la République, pour les besoins d'une procédure pénale, en vertu d'une réquisition prise à cette fin en application de l'article 77-1-1 du code de procédure pénale, la chambre de l'instruction n'a pas justifié sa décision (cassation au visa des textes préc., ensemble les art. 171 et 802 c. pr. pén.). »

[1841] V. *infra* n°1136.

[1842] Loi informatique et libertés modifiée par l'ordonnance du 12 décembre 2018 (*op. cit.* p.35) art. 101 : « Le responsable du traitement […] établit pour chaque traitement automatisé un journal des opérations […]. Les journaux des opérations de consultation et de communication permettent d'en établir le motif, la date […]. Ils permettent également […] d'identifier les personnes qui consultent ou communiquent les données […]. »

[1843] 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.

[1844] *Ibid,* art 25 : « journalisation ». Ce mot est synonyme de traçabilité.

Sur l'importance de la traçabilité des accès à une base de données, v. DELATTRE Laurent, *La gouvernance des données au coeur des audits en 2020*, ITforBusiness, 15 novembre 2019 : « […] les contrôles de sécurité autour des données et des ressources de stockage en vérifiant les contrôles mis en place, la visibilité et la traçabilité des accès ainsi que les sécurités en place pour protéger les informations où qu'elles soient. »

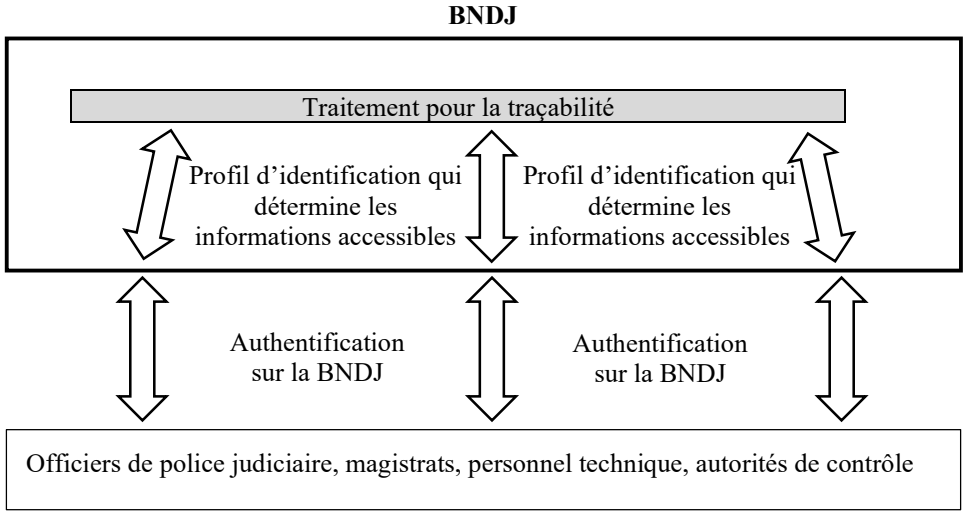


Illustration n°4 : Traitement pour la traçabilité des accès et des actions sur la BNDJ

1089. La proposition d'insertion dans le Code de procédure pénale. – Il est proposé d'insérer les dispositions visant à créer la BNDJ au sein du titre IV du livre I du Code de procédure pénale. En effet, ce titre n'est pas entièrement consacré à des fichiers de police[1845], et comporte d'autres investigations numériques diverses[1846]. Un chapitre VIII pourrait donc être ajouté à ce titre, portant les principales dispositions régissant la BNDJ[1847].

Le projet de décret pris en application des dispositions relatives à la Base Nationale des Données Judiciaires en fait de même dans la partie règlementaire du même Code, en proposant d'introduire un chapitre IV dans le titre IV, relatif aux « dispositions communes, » qui est le pendant de la proposition pour la partie législative dont il est question ci-dessus[1848].

1090. La conservation du principe de séparation entre les informations sensibles. – Outre le fait de ne pas créer un nouveau fichier de police,[1849] la BNDJ doit impérativement

[1845] Chapitre II : Des fichiers de police judiciaire - Chapitre III : Des logiciels de rapprochement judiciaire - Chapitre VI : De la plate-forme nationale des interceptions judiciaires.
[1846] Chapitre Ier : De la mise au clair des données chiffrées nécessaires à la manifestation de la vérité - Chapitre V : De la géolocalisation - Chapitre VII : De l'enquête sous pseudonyme.
[1847] Annexe 2, proposition de loi, article 10 : « Le titre IV du livre Ier du Code de procédure pénale, est complété par un chapitre VIII ainsi rédigé […] ».
[1848] Annexe 4, projet de décret pris en application des dispositions relatives à la base nationale des données judiciaires, article premier : « Le titre IV du livre Ier de la partie réglementaire du Code de procédure pénale, est complété par un chapitre IV […] ».
[1849] V. *supra* n°1087.

maintenir l'étanchéité entre les informations constituant le cœur des traitements judiciaires actuellement physiquement séparés, c'est-à-dire celles qui concrétisent la finalité pour laquelle le traitement a été créé[1850]. Ces données sont, par exemple, celles relatives à des antécédents de violence ou de terrorisme[1851]. L'étanchéité entre les informations numériques du cœur des fichiers de police doit être maintenu car, dans le cas contraire, le profilage généralisé tant redouté[1852] deviendrait une réalité[1853]. Le chapitre 2 de la proposition de loi destiné à créer la BNDJ doit donc préserver le principe de séparation des différents traitements qu'elle est appelée à héberger. En effet, la BNDJ n'introduirait pas un nouveau régime qui viendrait se substituer aux règles prévues pour chaque traitement de données judiciaires. Ainsi, le nouvel article 230-48 du Code de procédure pénale tel qu'il est proposé, explicite clairement que « les conditions d'alimentation et de consultation prévues pour chaque traitement s'appliquent strictement[1854] ». Cette proposition de disposition matérialise la distinction entre les traitements de judiciaires, que la BNDJ n'a pas vocation à modifier en profondeur, et les données composant ces traitements sur lesquelles la présente étude s'appuie pour proposer une amélioration.

1091. Par ailleurs, les conditions d'alimentation et de consultation des traitements, qui se feraient au travers de la BNDJ en tant qu'outil technique, imposent que toute connexion à la BNDJ devrait se faire au travers d'une connexion sécurisée[1855], ce qui est matérialisé sur l'illustration n°4.

1092. Le mise en commun de certaines données. – La BNDJ a vocation à apporter un équilibre entre la préservation de la séparation des informations sensibles constituant le

---

[1850] V. *supra* n°975.

[1851] V. resp. le « fichier judiciaire national automatisé des auteurs d'infractions sexuelles ou violentes » ou le « fichier judiciaire national automatisé des auteurs d'infractions terroristes ».

[1852] V. *supra* n°969.

[1853] Sur la volonté de l'Etat français de proscrire un profilage automatique à partir des fichiers de police, v. CASTETS-RENARD Céline, *Réforme de la LIL et transposition de la directive à des fins de coopération policière et judiciaire pénale*, Dalloz IP/IT 2018 p.480 : « Compte tenu des enjeux sociaux et de la faiblesse de certains outils utilisés par exemple aux États-Unis (3), ce parti pris est heureux. Par ailleurs, tout profilage qui entraînerait une discrimination à l'égard des personnes physiques sur la base des données sensibles est interdit […]. »
Sur l'interdiction de procéder à un profilage automatique par la loi informatique et libertés modifiée, v. *supra* n°664.

[1854] Annexe 2, proposition de loi, article 10, nouvel art.230-48 : « La base nationale des données judiciaires est directement accessible, par l'intermédiaire d'un système de télécommunication sécurisé :
1° A l'ensemble des personnes prévues par les dispositions spécifiques à chaque traitement hébergé. Les conditions d'alimentation et de consultation prévues pour chaque traitement s'appliquent strictement. […] »

[1855] Pour la description précise de la sécurisation des accès, v. *infra* n°1117.

cœur des traitements judiciaires actuels, tout en permettant de mettre en commun certaines données telles que celles relatives à la domiciliation et aux coordonnées afin d'améliorer la fiabilité de ces informations dans l'ensemble des traitements.

1093. La notion d'interconnexion. – La mise en commun d'une donnée suppose qu'elle soit présente dans plusieurs traitements distincts. Ainsi, la mise à jour de l'information numérique correspondante dans l'un des traitements induit la mise à jour pour les autres traitements[1856]. En droit, cette opération technique renvoi à la notion d'interconnexion. La définition littéraire d'interconnexion[1857] montre que ce mot se réfère directement à la mise en relation d'entités. Le RGPD utilise la notion d'interconnexion au travers de la définition du mot « traitement[1858] », tandis que la loi informatique et libertés modifiée par l'ordonnance de décembre 2018 regroupe, dans son article 33, « les interconnexions, les rapprochements ou toutes autres formes de mise en relation avec d'autres traitements[1859] ».

1094. L'interdiction de l'interconnexion neutralisée par la mise en œuvre des consultations. – L'interconnexion entre les traitements judiciaires est, le plus souvent, interdite[1860]. Néanmoins, cette étanchéité, légalement imposée, est très relative puisque,

---

[1856] Par ex. : l'adresse ou l'évolution de la qualification.

[1857] Interconnexion : « [informatique] Mise en relation de diverses entités matérielles ou logicielles pour qu'elles travaillent ensemble. » *Source : Larousse.*

[1858] V. *supra* n°1072.

[1859] Loi informatique et libertés modifiée par l'ordonnance du 12 décembre 2018, art 33 : « 3° Le cas échéant, les interconnexions, les rapprochements ou toutes autres formes de mise en relation avec d'autres traitements. ».
Cet article est applicable lors de la création d'un traitement de données judiciaires faisant l'objet du titre III de la même loi (art. 89 : « […] si le traitement est mis en œuvre […] pour au moins l'une des finalités énoncées au premier alinéa de l'article 87, il est prévu […] dans les conditions prévues au I de l'article 31 et aux articles 33 à 36 […] »).

[1860] V. par ex. le fichier judiciaire national automatisé des auteurs d'infractions terroristes avec l'art. 706-25-13 du C. pr. pén. : « Aucun rapprochement ni aucune interconnexion, au sens de l'article 33 de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, ne peuvent être effectués […]. »
V. eg. le Casier judiciaire. C. pr. pén. art. 777-3 : « Aucune interconnexion au sens du 3° du I de l'article 33 de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ne peut être effectuée entre le casier judiciaire national automatisé et tout autre fichier ou traitement de données à caractère personnel détenus par une personne quelconque ou par un service de l'Etat ne dépendant pas du ministère de la justice. »
V. eg. le fichier judiciaire national automatisé des auteurs d'infractions terroristes. C. pr. pén. art. 706-25-13 : « Aucun rapprochement ni aucune interconnexion, au sens de l'article 33 de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, ne peuvent être effectués entre le fichier prévu à la présente section et tout autre fichier ou recueil de données nominatives détenu par une personne quelconque ou par un service de l'Etat ne dépendant pas du ministère de la justice, à l'exception du fichier des personnes recherchées pour l'exercice des diligences prévues à la présente section. »

dans les faits des croisements d'informations, réalisés « manuellement », peuvent être facilement pratiqués. En effet, des dispositions relatives aux traitements judiciaires prévoient que seuls des agents ou des militaires habilités[1861] peuvent accéder aux traitements[1862]. Or, dans les Section de Recherche des gendarmeries ou les services de Police Judiciaire au sein de la Police, ce sont les mêmes agents ou militaires qui sont habilités pour plusieurs traitements. Ainsi, il est facile, pour ces agents autorisés, à interroger les différents fichiers auxquels ils ont accès et à procéder à une interconnexion « manuelle » des données.

1095. L'un des objectifs, au travers de la création de la BNDJ, est donc d'officialiser une interconnexion encadrée et contrôlée, afin d'améliorer la qualité des informations qui sont communes à plusieurs fichiers de police. Pour cela, il est nécessaire de donner une existence légale et règlementaire à l'interconnexion entre les différents traitements concernés.

1096. La légalisation de l'interconnexion pour les données communes. – En conséquence, au sein de la proposition de loi créant la BNDJ, la notion d'interconnexion est utilisée et définie au travers d'une disposition précise[1863]. L'objectif « d'identité des informations » est l'un des apports principaux de la BNDJ, puisque des erreurs dans les données peuvent potentiellement nuire aux personnes fichées ou toujours fichées alors qu'elles ne devraient plus l'être. C'est pourquoi, un second article est introduit dans la proposition de loi pour légaliser le principe de mise à jour automatique[1864], sous le contrôle du juge.

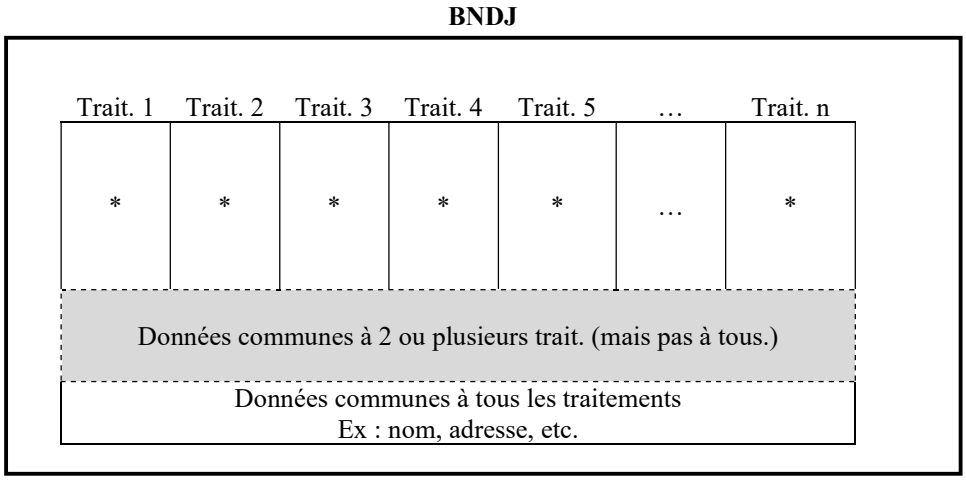
[1861] Sur la stricte application de l'obligation d'être habilité pour les agents ou militaires accédant à des traitements judiciaires, v. Civ. 1ère 17 oct. 2018 n°17-16.852, ECLI:FR:CCASS:2018:C100961.
DAOUD Emmanuel et LEONE Thomas, *Fichiers Visabio et FAED : l'accès par une personne habilitée ne se présume pas et l'utilisation d'un mot de passe personnel n'est pas une garantie suffisante*, Dalloz IP/IT 2019 p.118 : « Les hauts magistrats reprochent aux termes d'un attendu de principe limpide que l'accès aux fichiers ait été confirmé « sans rechercher, comme il le lui était demandé, s'il résultait des actes de la procédure, notamment des mentions faisant foi jusqu'à preuve du contraire, du procès-verbal contenant le résultat de la consultation des fichiers, que le fonctionnaire de police les ayant consultés était expressément habilité à cet effet ».

[1862] V. *supra* n°707.

[1863] Annexe 2, proposition de loi, article 10, nouvel art. 230-49 : « Une interconnexion technique au sens du 3° du I de l'article 33 de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés est mise en œuvre afin de garantir l'identité des informations saisies entre les différents traitements de données à caractère personnel hébergés. »

[1864] *Ibid,* article 10, nouvel article 230-50 : « Toute mise à jour ou tout effacement des données personnelles stockées dans l'un des traitements hébergés, ordonné par l'autorité judiciaire compétente ou légalement prévue, est répercuté dans l'ensemble des autres traitements hébergés. »

1097. L'équilibre entre la mise en commun de certaines données et le cloisonnement des informations sensibles. – L'illustration n°5 reprend, visuellement, le deuxième rôle de la BNDJ comportant des données mises en commun et celles constituant le cœur de chaque traitement judiciaire spécialisé qui doivent rester cloisonnées.



(*) Données spécifiques aux traitements judiciaires

Illustration n°5 : Données communes /données séparées au sein de la BNDJ

1098. Conclusion du sous-paragraphe I : l'équilibre entre mise en commun et étanchéité de données. – La Base Nationale de Données Judiciaires serait une entité technique permettant de regrouper des données communes à plusieurs traitements judiciaires, tout en conservant le principe de séparation entre ces derniers[1865]. En effet, le fait d'enregistrer les informations dans une même base de données ne préjuge en rien du fait que plus aucun cloisonnement n'existerait entre différents fichiers de police. La BNDJ permettrait de regrouper les données qui sont communes à plusieurs traitements, ce qui serait une source très importante d'amélioration de la qualité des informations stockées dans les traitements judiciaires. Une proposition de loi[1866] et un projet de décret[1867] permettraient de donner une existence légale à la BNDJ.

1099. De plus, la BNDJ, en regroupant dans une même entité informatique plusieurs traitements judiciaires, faciliterait le contrôle de ces derniers.

[1865] V. *supra* n°1090.
[1866] Annexe 2, proposition de loi visant à améliorer l'efficacité et à renforcer les garanties des traitements de données en procédure pénale.
[1867] Annexe 4, projet de décret pris en application des dispositions relatives à la base nationale des données judiciaires, article premier.

II – Un contrôle facilité et renforcé

1100. La centralisation de la localisation et l'homogénéisation technique pour faciliter les contrôles. – La multiplication des traitements judiciaires, éparpillés au sein de structures différentes nuit à la qualité et l'effectivité des contrôles prévus[1868]. La création d'une BNDJ regroupant plusieurs fichiers de police dans une même entité informatique, tout en maintenant la séparation entre les informations constituant le cœur des traitements mis en œuvre, permettrait de faciliter et de renforcer les contrôles de ces derniers. En effet, d'une part, il est évidemment plus aisé d'exercer un audit de ces traitements si l'autorité en charge des contrôles ne doit se rendre qu'en un seul lieu plutôt qu'en plusieurs et, d'autre part, si la mise en œuvre technique de ces traitements est homogénéisée. Sur ce dernier point, l'autorité de contrôle doit comprendre un seul fonctionnement pour un ensemble de fichiers de police plutôt qu'autant de modalités techniques que de traitements.

1101. Comme précédemment évoqué, l'amélioration des contrôles des traitements est indispensable pour le suivi, notamment des effacements et des mises à jour qui sont actuellement fortement déficients[1869].

1102. Le modèle de la PNIJ. – En matière de contrôle, il existe actuellement de multiples régimes qui diffèrent d'un traitement à un autre. Tout au plus, l'intervention d'un magistrat du parquet placé hors hiérarchie est fréquente[1870]. En revanche, la PNIJ peut servir de modèle[1871] car son fonctionnement est transparent et fait l'objet de rapports réguliers[1872]. Ainsi, dans la proposition de loi relative à la BNDJ, un nouvel article 230-52, relayé par les nouveaux articles R40-60 et R40-61 issus du projet de décret d'application, viendrait créer la structure de contrôle en lui confiant une mission générale en ce sens. Cette structure serait donc composée d'un contrôleur assisté d'un comité[1873], à l'identique de ce qui existe pour la PNIJ.

[1868] V. *supra* n°1025.
[1869] V. *supra* n°1013.
[1870] V. *supra* n°1027.
[1871] V. *supra* n°1028.
[1872] *Op. cit.* p.35, IMBERT-QUARETTA Mireille, *1er rapport d'activité.* Madame IMBERT-QUARETTA est la contrôleure de la PNIJ.
[1873] Annexe 2, proposition de loi, article 10, nouvel art. 230-52 : « Art. 230-52. - La base nationale des données judiciaires est placée sous le contrôle d'une personnalité qualifiée, assistée par un comité, selon des conditions définies par décret. »

1103. La nécessité de renforcer le contrôle des mises à jour. – Le nouvel article R40-60 tel qu'il est proposé, confierait un rôle central au contrôleur de la BNDJ dans les processus de mise à jour des informations contenues dans l'ensemble des traitements hébergés[1874]. Cette intervention ne ferait évidemment pas obstacle aux prérogatives de la CNIL telles qu'issues de l'entrée en vigueur du RGPD et de la directive relative aux traitements de données judiciaires[1875].

1104. Les conséquences sur le régime des traitements hébergés. – Pour l'ensemble des traitements qui seraient concernés par la mise en relation de certaines données, des dispositions spécifiques doivent être prévues. L'objectif est que le contrôleur de la BNDJ et le comité qui l'assiste puissent être au cœur de toutes les actions nécessitant un contrôle fort. En premier lieu, le contrôleur et le comité devraient être systématiquement informés des refus de suppression de fiches lorsque cette possibilité est offerte au procureur de la république, et être sollicité pour apporter leur expertise, par le juge judiciaire[1876] qui serait éventuellement saisi par une personne qui contesterait le refus d'effacement des données le concernant. En deuxième lieu, il serait impératif que leur soient communiqués les rapports annuels lorsqu'ils sont prévus. Enfin, en troisième et dernier lieu, leurs possibilités de contrôle devraient être effectives, ce qui ne peut se faire que par des dispositions législatives et règlementaires entérinant ces trois points.

1105. Ainsi, tous les traitements judiciaires qui seraient hébergés dans la BNDJ devraient prévoir une disposition autorisant de tels contrôles[1877].

1106. Conclusion du sous-paragraphe II : un contrôle facilité et renforcé. – La proposition de créer la BNDJ doit nécessairement comporter la création d'une structure de contrôle efficace. Cette dernière serait composée d'un contrôleur et d'un comité. Cette

---

[1874] Annexe 4, article premier, nouvel article R40-60 : « […] Cette personnalité est informée de toutes les demandes d'accès ou de rectification relatives aux informations propres à la base nationale des données judiciaires ainsi qu'aux informations contenues dans les traitements automatisés de données à caractère personnel hébergés. […] »

[1875] *Ibid.* « […] Les pouvoirs qui lui sont confiés s'exercent sans préjudice du contrôle exercé par la Commission nationale de l'informatique et des libertés en application des dispositions et selon les modalités prévues par les articles 101,105,107 et 108 de la loi n°78-17 du 6 janvier 1978. »

[1876] Depuis la modification de l'article 230-8 du C. pr. pén. 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, c'est le juge judiciaire qui est compétent pour connaître des contentieux liés aux effacements des données.
Le tribunal des conflits a confirmé cette situation. T. conf. 8 oct. 2018, n°C4134, M. G. c/ ministère de la Justice.

[1877] V. *infra* n°1167.

structure de contrôle ainsi composée, serait en pleine capacité de pouvoir vérifier que les mises à jour et les effacements des données seraient bien réalisées. De même, lorsque l'autorité judiciaire ordonnerait le maintien de certaines informations, les raisons en seraient justifiées et exceptionnelles. D'une manière générale, c'est un contexte d'une plus grande transparence sur la nature des données collectées et des possibilités d'exploitation autorisées qui serait créé par la BNDJ grâce à un contrôle amélioré et effectif. Certes, il ne serait pas confié au contrôleur de la BNDJ un pouvoir de contrainte, mais il pourrait, dans son rapport annuel, aisément dénoncer des excès qu'il constaterait et pourrait alors proposer des modifications pertinentes. L'apport de la BNDJ pour le respect des libertés individuelles serait ici déterminant puisque l'hébergement regroupé de traitements judiciaires faciliterait énormément les contrôles, notamment parce que le contrôleur pourrait en prendre l'initiative.

1107. Conclusion de la section 1 : la proposition du regroupement des données par la création de la BNDJ. – La possibilité de procéder à un regroupement mesuré de certaines données présentes dans différents traitements judiciaires améliorerait la qualité des données et, par là-même, l'efficacité de l'enquête et le respect des libertés individuelles. La proposition de créer la Base Nationale de Données Judiciaires répond à cet objectif. La BNDJ serait à la fois une entité juridique et une entité technique, à l'identique de la PNIJ qui est à la fois un traitement judiciaire et un service opérationnel[1878]. La proposition de créer la BNDJ repose sur trois étapes. La première consiste à étudier le cadre légal et réglementaire qu'il serait nécessaire de mettre en œuvre pour créer une telle entité[1879]. La deuxième étape énonce des règles générales pour les données qui pourraient être regroupées au sein de la BNDJ.

1108. Une troisième étape est nécessaire pour définir les critères qui définiraient quels sont les traitements judiciaires pour lesquels il est pertinent de procéder à un certain rapprochement des données et selon quelles modalités. Cette étape fait partie de l'étude du régime de la BNDJ qui est proposé.

[1878] V. *supra* n°687.
[1879] V. *supra* n°1084.

Section 2. La proposition d'un régime pour la BNDJ

1109. L'étude du régime permettant à la BNDJ de fonctionner. – Après avoir énoncé les règles générales qui pourraient permettre la création de la BNDJ, l'étude doit se poursuivre en proposant un régime de fonctionnement pour celle-ci. En premier lieu, un cadre légal relatif au fonctionnement de cette entité informatique doit être proposé *(§1)*. En second lieu, des critères pour définir les fichiers appelés à être hébergés dans la BNDJ ou liés à celle-ci doivent être énoncés, ce qui nécessiterait que le régime des traitements judiciaires répondant à ces critères doit être étudié *(§2)*.

§1. Le régime de la mise en œuvre opérationnelle de la BNDJ

1110. Le socle de mise en œuvre de la BNDJ. – Le fonctionnement opérationnel de la BNDJ suppose de s'intéresser à deux niveaux différents. D'une part, les accès à cette entité informatique doivent être encadrés *(I)*. D'autre part, le cadre légal relatif à la gestion des informations numériques collectées et enregistrées doit être strictement défini *(II)*.

I – Le régime des accès à la BNDJ

1111. L'encadrement des différents accès. – Il existe deux types d'accès distincts. En effet, les accès des opérateurs mettant en œuvre la BNDJ *(A)* sont différents, en termes de besoins et de contraintes techniques, des accès des utilisateurs ayant besoin d'accéder aux informations numériques enregistrées, dans le cadre de leur travail et de leur fonction *(B)*.

A. Le régime des accès des administrateurs de la BNDJ

1112. L'évidence du service du Casier judiciaire. – Pour que la BNDJ puisse exister, il faudrait qu'une infrastructure informatique[1880] existe. Actuellement, le *cloud*[1881] prenant de plus en plus d'importance, ce n'est pas la localisation physique de cette infrastructure qui compte, mais les personnes à qui sont confiés les accès pour son fonctionnement. Dans le jargon informatique, ce sont les administrateurs[1882].

[1880] L'infrastructure couvre un ensemble important d'équipements : les ordinateurs, les unités de stockage, des équipements réseaux assurant la communication avec l'extérieur, etc. Pour gérer un tel projet technique, il existe des services spécialisés au niveau de l'Etat : v. *supra* n°919.
[1881] V. *supra* n°221.
[1882] Que l'on peut distinguer en administrateur « réseau » (BOUCQ Isabelle, *Profession administrateur réseau*, Micro Hebdo, 2 mars 2005) et administrateur base de données dans le cas de la BNDJ.

1113. Comme précédemment expliqué, le service du Casier judiciaire joue un rôle de plus en plus important dans les traitements judiciaires hautement sensibles[1883]. Il serait donc cohérent que la mise en œuvre opérationnelle et la supervision informatique de l'infrastructure hébergeant la BNDJ lui soient confiées, notamment en raison des moyens techniques et humains qui composent ce service[1884] et pour que les budgets consacrés par l'Etat à la sécurisation des traitements judiciaires ne soient pas dispersés[1885]. Le chapitre deux, de la proposition de loi visant à améliorer l'efficacité et à renforcer les garanties des traitements de données en procédure pénale[1886], destiné à créer et mettre en œuvre la BNDJ, retranscrit cette mission du service du Casier judiciaire[1887].

1114. Un meilleur rattachement au juge. – L'extension de l'intervention du service du Casier judiciaire pour l'ensemble des fichiers de police appelés à être hébergés par la BNDJ représenterait une amélioration importante du respect des libertés individuelles des personnes fichées. En effet, de nombreux traitements accessibles en enquête sont actuellement sous le contrôle technique de services de police judiciaire. Ce sont donc des policiers ou des gendarmes qui ont le pouvoir d'administration, au sens informatique du terme[1888]. C'est, notamment, le cas du traitement d'antécédents judiciaires, ce qui permet aux enquêteurs de pouvoir procéder à des fouilles de données directement dans la base[1889]. Placer le TAJ sous la responsabilité du service du casier judiciaire reviendrait, de fait, à supprimer ce type de croisements de données réalisés en dehors de toute justification légale[1890]. Plus généralement, le service du casier judiciaire « est dirigé par un magistrat de l'administration centrale du ministère de la Justice […] ». Même si ce magistrat est

---

[1883] V. *supra* n°641.
[1884] Pour un aperçu des moyens techniques et du fonctionnement du service du Casier judiciaire, v. Libération, *La mémoire longue conservation de la justice*, 12 septembre 2013.
[1885] V. *supra* n°1043.
[1886] V. *supra* n°1079.
[1887] Annexe 2, proposition de loi, article 10, nouvel art. 230-47 : « […] il est créé une base nationale des données judiciaires tenue par le service du casier judiciaire sous l'autorité du ministre de la justice. »
[1888] Sur les risques liés au potentiel d'intervention des administrateurs sur les bases de données, v. COHEN Jo, *Données personnelles,* PUBLINET Sécurité Informatique, n°418, 3 juin 2014, entretien avec Laurent DELAPORTE : « Les menaces internes sont plus difficiles à appréhender. […] Une entreprise qui dispose de plusieurs bases de données […] doit donner des clés de chiffrement à chaque administrateur de base de données, ce qui augmente les risques. »
[1889] V. *supra* n°647.
[1890] Sur la différence de crédibilité et de fiabilité des informations entre celles du Casier judiciaire et celles du TAJ (anciennement STIC et JUDEX : v. *supra* n°154.), v. *ibid.* Libération, *La mémoire longue conservation de la justice*, 12 septembre 2013 : « [Le casier judiciaire :] Rien à voir avec les fichiers de police et de gendarmerie comme le Stic ou autre Judex, décriés pour leur manque de crédibilité et de confidentialité. »

rattaché à une administration[1891], il y a là un renforcement du lien avec les décisions des juges du siège[1892], par opposition aux traitements qui sont actuellement placés sous le contrôle d'un magistrat du parquet, même hors hiérarchie[1893].

1115. Une complémentarité avec le contrôle de la BNDJ. – Le rôle de ce magistrat est différent de celui de la personnalité prévue par le nouvel article 230-52[1894]. Le magistrat qui dirige le service du Casier judiciaire est chargé d'une fonction opérationnelle de mise en œuvre et de fonctionnement des traitements de données qui sont confiés au service, tandis que la personnalité prévue au nouvel article 230-52, assistée d'un comité, a une mission de contrôle et de conseil, à l'identique de ce qui existe actuellement pour la PNIJ[1895].

1116. Conclusion du sous-paragraphe A : le cadre légal des accès des administrateurs de la BNDJ. – Pour exister, un traitement judiciaire nécessite une infrastructure informatique. Celle-ci nécessite d'être administrée par du personnel technique pour fonctionner. Le service du Casier judiciaire prend, depuis quelques années, de plus en plus d'importance en matière d'administration de traitements judiciaires, puisque plusieurs fichiers sensibles lui ont été donnés. C'est donc à ce service que la présente étude propose de confier la responsabilité technique de la BNDJ.

[1891] Sur l'intégration du magistrat responsable du service du Casier judiciaire dans l'organisation administrative : v. Ouest-France Vendée, 5 mai 2012, *Départ du procureur de la République vers Nantes* : « Cette fois, le magistrat originaire de Machecoul prend un poste de sous-directeur, chef du service du casier judiciaire national. Il dépendra de la direction des affaires criminelles et des grâces. »
[1892] V. *supra* n°1076.
[1893] V. *supra* n°1027.
[1894] V. *supra* n°1102. Annexe 2, proposition de loi, article 10.
[1895] V. *supra* n°1028.

B. Le régime des accès des utilisateurs de la BNDJ

1117. Les utilisateurs des traitements de données. – Toutes les entités de la chaîne judiciaire (tribunaux, gendarmeries, police nationale, douanes) auraient potentiellement besoin d'accéder aux informations contenues dans certains des traitements judiciaires appelés à être hébergés par la BNDJ. Cette connexion serait obligatoirement réalisée à distance puisque l'intérêt de tels fichiers est d'être centralisé, ce qui signifie que l'infrastructure informatique est géographiquement éloignée[1896]. Le nouvel article 230-47 reprend des formulations déjà existantes pour certains traitements[1897] afin de maintenir une homogénéité dans le Code de procédure pénale, et impose ainsi un cadre légal de sécurité aux connexions à la BNDJ, tout en explicitant le fait que celles-ci soient réalisées à distance, en employant l'expression « moyen de télécommunication ». L'encadrement des personnes autorisées à se connecter est également retranscrit en renvoyant aux dispositions propres à chaque traitement[1898], ce qui est conforme avec l'un des objectifs de la BNDJ de ne pas se substituer aux fichiers de police actuels[1899]. Seul l'accès de la personne en charge du contrôle de la BNDJ est ajouté afin de rendre sa mission possible[1900].

1118. La convergence entre le cadre légal et l'infrastructure informatique. – Comme précédemment expliqué, la création d'une BNDJ ne serait possible que si les outils informatiques permettraient de mettre en œuvre efficacement le cadre juridique[1901], notamment en matière de protection des données judiciaires, hautement sensibles par

[1896] V. *supra* n°1112.
[1897] V. par ex. le fichier judiciaire national automatisé des auteurs d'infractions sexuelles ou violentes, C. pr. pén. art. R53-8-39 : « L'enregistrement et la consultation du fichier se font par l'intermédiaire de moyens de télécommunication sécurisés. La transmission de données entre le service gestionnaire du fichier et le ministère de l'intérieur se fait par un moyen informatique sécurisé. »
[1898] Annexe 2, proposition de loi, article 10, nouvel art. 230-48 : « La base nationale des données judiciaires est directement accessible, par l'intermédiaire d'un système de télécommunication sécurisé :
1° A l'ensemble des personnes prévues par les dispositions spécifiques à chaque traitement hébergé. Les conditions d'alimentation et de consultation prévues pour chaque traitement s'appliquent strictement. […]. »
[1899] V. *supra* n°1087.
[1900] Annexe 2, proposition de loi, article 10, nouvel art. 230-48 : « La base nationale des données judiciaires est directement accessible, par l'intermédiaire d'un système de télécommunication sécurisé :
[…]
2° A la personne qualifiée ainsi qu'aux membres du comité prévus à l'article 230-52, pour le strict exercice de leur mission. »
[1901] V. *supra* n°1066.

définition[1902], ainsi qu'en préservant le maintien des règles d'accès cloisonnés aux informations enregistrées[1903].

1119. Un double degré de connexion à la BNDJ. – Le fort degré de sécurisation d'un système d'information n'est le plus souvent qu'une affaire de moyens alloués[1904]. Dans le cas de la BNDJ, un double degré de connexion constituerait une solution pour sécuriser l'accès aux données[1905]. Ces deux étapes sont matérialisées sur l'illustration n°4[1906].

1120. L'authentification à la BNDJ. – Dans un premier temps, l'origine de la connexion doit faire l'objet d'une authentification[1907]. Une technique élémentaire consiste à authentifier le site[1908] depuis lequel émane la connexion, par le biais d'un filtrage de la plage des adresses IP[1909]. Néanmoins, cette façon de procéder engendre une restriction importante car cela induit que les travailleurs à distance[1910] ou en mission à l'extérieur de leur bureau, comme les officiers de police judiciaire lorsqu'ils sont sur le terrain, ne peuvent pas consulter les fichiers avec ce type de filtrage. Dans de nombreux domaines professionnels, cette méthode d'authentification est usitée[1911].

1121. Toutefois, dans le cas des gendarmes et des policiers qui vient d'être évoqué, c'est-à-dire lors de leurs interventions sur le terrain, les besoins d'identification rapide d'un individu sont une nécessité. Pour procéder à cette identification, l'accès aux traitements de données est évidemment requis. Cette préoccupation est prise en compte par les autorités publiques puisque le développement de moyens numériques mobiles pour les forces de l'ordre sur le terrain fait actuellement partie d'un projet de recherche

---

[1902] Les informations contenues dans les fichiers de police sont considérées comme sensibles suite à « un bras de fer » entre la CNIL et le pouvoir exécutif qui s'est engagé en 1981 : GAUTRON Virginie, *Fichiers de police*, Dalloz Répertoire de droit pénal et de procédure pénale, mars 2019, généralités al. 13.
[1903] V. *supra* n°1090.
[1904] Sur la protection technique des systèmes d'information, v. *supra* n°1043.
[1905] Sur les techniques de sécurisation de gestion des identités pour accéder à un système d'information, v. Silicon, *Gestion des identités et des accès : comment choisir entre les solutions logicielles et le Saas*, Silicon site web, 1 avril 2019.
[1906] V. p.35
[1907] V. les normes ISO 2700x (v. *supra* n°1036.).
[1908] Ou l'entité car, par exemple, dans un Hôtel de police de taille importante, seuls quelques services peuvent être habilités à accéder à un traitement judiciaire de données et donc à la BNDJ.
[1909] *Internet Protocol* : l'adresse qui est attribuée pour se connecter à un réseau informatique utilisant Internet.
[1910] De nombreux magistrats placés travaillent des dossiers depuis leur domicile lorsqu'ils n'ont pas d'audience.
[1911] Dans le monde universitaire, certaines ressources numériques mises à disposition par la Bibliothèque Universitaire ne sont accessibles que lorsque l'on est connecté sur le réseau de l'université. Certains éditeurs imposent cela pour mieux encadrer les utilisateurs de leurs ressources.

informatique[1912]. Celui-ci permettra certainement de proposer de nouvelles méthodes alliant sécurité et souplesse dans l'authentification d'un terminal.

1122. L'identification au sein de la BNDJ. – Dans un second temps, après l'authentification du terminal, l'utilisateur s'identifie au travers d'un mécanisme qui peut être aussi classique qu'avec un *login* et un mot de passe ou par le biais d'une carte professionnelle[1913].

1123. A ce stade l'utilisateur est connecté à la BNDJ, mais il n'a encore accès à aucune donnée. C'est alors qu'interviennent les droits d'accès par profil[1914] puisque, de base, il est normal qu'un officier de police judiciaire ait accès au Traitement d'Antécédents Judiciaires (TAJ) ou un magistrat à Cassiopée. En revanche, l'accès à des traitements dont la consultation est encadrée doit être renforcé par des techniques informatiques largement répandues telles que l'utilisation d'un code à usage unique[1915], par exemple. Il s'agit d'un deuxième niveau d'identification qui préserve le cloisonnement des informations des traitements sensibles au sein de la BNDJ[1916]. Ce code pourrait être délivré par le magistrat en charge du dossier[1917]. Il présente le double avantage, d'une part, de se prémunir contre des consultations non autorisées et, d'autre part, d'associer la consultation autorisée au numéro de la procédure concernée. Cette nouvelle traçabilité est un apport aux libertés individuelles car il permet de s'assurer, *a posteriori*, que les données extraites n'ont pas été utilisées dans une autre procédure ou à mauvais escient[1918]. Dès lors que ce deuxième niveau d'identification est opéré, la consultation, la saisie d'informations, l'effacement, ainsi que toute intervention sur les données peuvent se dérouler dans les mêmes conditions qu'avec la situation actuelle des traitements judiciaires physiquement séparés.

[1912] « Policier 2025 ». Les chercheurs en informatique parlent « d'authentification multi-facteurs ».

[1913] Sur l'évolution et l'aspect critique des techniques d'identification, v. DURAND André, *Gestion des identités et des accès : les grandes tendances de 2020*, Silicon, 6 janvier 2020 : « […] le concept traditionnel de périmètre de sécurité a vécu, et la notion d'identité est désormais au cœur de la cyber sécurité. »

[1914] V. illustration n°4, p.35.

[1915] Un code à usage unique est fréquemment utilisé, notamment dans le domaine bancaire, pour autoriser une transaction. L'exemple le plus fréquent consiste à envoyer ce code, valable pour une seule opération, sur le téléphone portable de la personne titulaire du compte courant, afin de finaliser le paiement à distance.

[1916] Sur le double degré d'authentification et l'usage du code unique, v. O1NET, *Sécurisez l'accès à votre compte UBUNTU*, 01net, 6 février 2019.

[1917] En fonction des traitements, il peut s'agir du Juge d'instruction, du procureur ou du Juge des libertés et de la détention.

[1918] L'Est Républicain, *Un officier de police suspendu*, Lorraine, mardi 26 février 2019, p.6 : « Il a été aussi mis en examen pour un troisième délit : le détournement de fichiers de police à des fins personnels. Les enquêteurs auraient en effet découvert qu'il avait consulté des fichiers pour se renseigner sur son ancienne petite amie et pour identifier les propriétaires de voitures dont il aurait relevé les plaques devant le domicile de son ex. »

1124. La traçabilité des accès. – L'ensemble de ces différentes étapes d'accès aux données, doit faire l'objet d'une traçabilité complète. Il s'agit d'une caractéristique essentielle de la BNDJ[1919] pour faciliter et améliorer les contrôles. En effet, actuellement, une telle traçabilité commence à se mettre en place, mais elle ne concerne pas l'ensemble des traitements judiciaires comme le reconnaissent les utilisateurs[1920]. L'illustration n°4 permet de visualiser cette partie de la BNDJ et son lien avec les accès[1921].

1125. Conclusion du sous-paragraphe I : le cadre légal des accès à la BNDJ. – Les accès à la BNDJ sont des éléments essentiels du régime de celle-ci, puisque les informations appelées à y être hébergées sont particulièrement sensibles. En premier lieu, les accès techniques, inhérents au fonctionnement de la BNDJ, pourraient être confiés aux équipes du service du Casier judiciaire afin de s'appuyer sur des compétences reconnues, et placés sous la responsabilité d'un magistrat. En deuxième lieu, les accès des utilisateurs dument habilités à intervenir sur les informations par les dispositions relatives aux traitements appelés à être hébergés par la BNDJ, pourraient être, techniquement, décomposés en deux étapes afin de répondre à des exigences de sécurité optimale. Un premier degré d'identification permettrait la connexion à la BNDJ, tandis qu'une seconde identification conditionnerait l'accès aux traitements et donc aux données. En troisième lieu, les accès du personnel technique et des utilisateurs devraient faire l'objet d'une traçabilité complète.

II – Le régime de la gestion des données

1126. L'objectif d'améliorer les droits des personnes fichées. – La création de la Base Nationale de Données Judiciaires permettrait de mettre en commun certaines données, communes à plusieurs traitements judiciaires, tout en maintenant une séparation constituant le cœur de ces fichiers[1922]. Néanmoins, la proposition de création de la BNDJ doit comporter des améliorations pour la gestion de toutes les données enregistrées dans les traitements qui seraient hébergés par la BNDJ, afin de renforcer le respect des libertés individuelles, notamment lors des consultations. L'objectif est de totalement proscrire

[1919] V. *supra* n°1087.
[1920] VEDEL Renaud, *Le rôle des fichiers dans l'action opérationnelle des services de sécurité intérieure*, Dalloz AJ pénal 2007 p.64 : « La consultation de la grande majorité des fichiers de police s'effectue désormais par une interface d'accès qui journalise accès et consultation de manière individualisée, par poste et par agent ; elle est désignée par l'acronyme CHEOPS. »
[1921] V. p.35
[1922] V. *supra* n°1090.

l'extraction de données relatives à des témoins ou des victimes lors de la consultation des traitements judiciaires.

1127. L'introduction d'un code dans le respect de la nouvelle loi informatique et libertés. – Pour la gestion des informations au sein de la BNDJ, il conviendrait de s'inspirer des codes utilisés dans le Traitement d'Antécédents judiciaires[1923] pour créer trois catégories clairement distinguées. Une première regrouperait les personnes mises en cause, condamnées ou recherchées[1924]. Une deuxième serait relative aux témoins tandis que la troisième regrouperait les victimes. Un tel code respecterait les dispositions de la nouvelle loi informatique et libertés qui imposent au responsable de traitement « d'établir une distinction claire entre les données à caractère personnel de différentes catégories de personnes concernées[1925] ». Cependant, la procédure pénale telle qu'elle est actuellement conçue en France, ne permet pas de distinguer les personnes suspectées des personnes condamnées, au sein des traitements judiciaires. Au contraire, la procédure privilégie l'efficacité du « fichage[1926] » en autorisant l'alimentation des fichiers le plus tôt possible[1927]. Cette façon de procéder permet à des officiers de police judiciaire de pouvoir identifier un suspect déjà mis en cause dans d'autres dossiers, au travers des informations contenues dans l'un de ces traitements, sans attendre qu'un jugement soit prononcé pour les premiers faits. Il y a là un danger potentiel pour la protection des victimes et des témoins, puisque l'exploitation des données enregistrées dans les traitements judiciaires peuvent permettre aux enquêteurs de procéder à des corrélations d'informations de personnes qui ne sont ni délinquants ni criminels[1928].

[1923] V. *supra* n°1019. Un code est affecté afin de répartir les personnes fichées en « personne mise en cause », victime ou témoin.

[1924] La catégorie des personnes recherchées comporte les disparitions inquiétantes ainsi que toutes les données relatives à un cadavre découvert et dont on ne connait pas l'identité.

[1925] Loi informatique et libertés modifiée par l'ordonnance du12 décembre 2018, art. 98 : « […]
1° Les personnes à l'égard desquelles il existe des motifs sérieux de croire qu'elles ont commis ou sont sur le point de commettre une infraction pénale ;
2° Les personnes reconnues coupables d'une infraction pénale ;
3° Les victimes d'une infraction pénale ou les personnes à l'égard desquelles certains faits portent à croire qu'elles pourraient être victimes d'une infraction pénale ;
4° Les tiers à une infraction pénale, tels que les personnes pouvant être appelées à témoigner lors d'enquêtes en rapport avec des infractions pénales ou des procédures pénales ultérieures, des personnes pouvant fournir des informations sur des infractions pénales ou des contacts ou des associés de l'une des personnes mentionnées aux 1° et 2°. »

[1926] V. *supra* n°967.

[1927] Par ex., le fichier automatisé des empreintes digitales, le fichier judiciaire national automatisé des auteurs d'infractions sexuelles ou violentes, le fichier judiciaire national automatisé des auteurs d'infractions terroristes, etc.

[1928] Les traitements judiciaires concernent notamment des personnes qui ne sont pas suspectées mais qui font parties de l'entourage d'un suspect. V. *supra* n°645.

1128. Un code dédié aux utilisateurs. – Une quatrième catégorie devrait être ajoutée pour l'ensemble des utilisateurs qui interviennent sur les données : il s'agit des données de traçabilité[1929]. La prise en compte des utilisateurs permettrait de ne pas négliger le traitement de données à caractère personnel qui les concernent et de pouvoir mettre la BNDJ en conformité avec les obligations qui incombent à l'Etat en matière de journalisation des informations collectées lors des manipulations et consultations des utilisateurs[1930].

1129. L'aspect essentiel de ce code est retranscrit dans le chapitre deux, de la proposition de loi visant à améliorer l'efficacité et à renforcer les garanties des traitements de données en procédure pénale, dédié à la BNDJ, puisqu'il y est fait référence dès le premier article qui est proposé[1931].

1130. Un code pour améliorer les droits des personnes fichées. – La gestion de ce code en tant que partie intégrante de la BNDJ est l'un des atouts susceptibles d'améliorer la protection de la vie privée et le respect des libertés individuelles. En effet, seul le code correspondant aux personnes mises en cause ou précédemment condamnées, ou recherchées, serait susceptible d'autoriser une consultation sur l'intégralité des données au sein du fichier interrogé. Ainsi, aucune donnée relative aux victimes ou aux témoins ne devrait figurer dans le résultat d'une investigation réalisée dans le cadre d'une enquête au sein des traitements[1932]. Les victimes et les témoins ne devraient apparaître que lors de la consultation du dossier de procédure (grâce au numéro géré par Cassiopée[1933]) dans lequel ils ont été entendus ou que leurs noms apparaîtraient.

1131. Les mises à jour de ce code par les autorités judiciaires au cours d'une procédure seraient cruciales puisque, par exemple, une personne initialement mise en cause, puis dont le dossier se terminerait, à son égard, par un classement sans suite, un non-lieu, une

---

[1929] V. *supra* n°1087.

[1930] V. *infra* n°1135.

[1931] Annexe 2, proposition de loi, article 10, nouvel art. 230-47 : « Un code unique est associé aux personnes faisant l'objet d'un enregistrement dans l'un ou plusieurs de ces traitements, aux fins de déterminer si elles y sont présentes :
a° en qualité de personnes mises en cause, condamnées ou recherchées,
b° en qualité de témoins,
c° en qualité de victimes.
Un quatrième code est affecté aux agents, militaires et autre personnel habilité à accéder et opérer sur les données, dans le respect de la traçabilité prévue à l'article 230-51. »

[1932] V. *supra* n°633. Certains traitements permettent des recherches par mots clés qui peuvent aboutir à des résultats faisant apparaître le nom de personnes inconnues jusque-là dans la procédure. Il est essentiel que ces résultats ne puissent pas faire apparaître le nom des catégories « témoins » et « victimes ».

[1933] V. *infra* n°1173.

relaxe ou un acquittement devrait voir, instantanément, son code évoluer vers celui de « témoin »[1934]. Il devrait en être de même pour un cadavre qui serait classifié dans la catégorie des personnes recherchées. Ce classement au début d'un dossier permettrait que l'intégralité des données le concernant apparaissent dans toutes les consultations autorisées. Les conditions seraient alors optimales pour éclaircir les faits ayant conduit à son décès. Dès que celui-ci serait élucidé et qu'il apparaîtrait que ce cadavre n'est qu'une victime, alors le changement de code devrait intervenir immédiatement. Il convient, en effet, de rappeler que les données génétiques des personnes mises en cause ou précédemment condamnées peuvent faire l'objet de rapprochement d'ordre familial[1935]. Il serait donc primordial que le changement de code soit opéré afin que la famille de cette victime ne puisse pas faire l'objet de rapprochements génétiques lors d'une enquête ultérieure.

1132. L'importance de la traçabilité des mises à jour du code. – L'introduction d'un code permettant de limiter les recherches au sein des traitements hébergés sur les données des personnes mises en cause ou condamnées, est un élément essentiel de la gestion des informations au sein de la BNDJ. Dès lors, la mise à jour de ce code est critique pour que les droits des personnes présentes dans les fichiers de police soient respectés. Ainsi, il est nécessaire que la proposition de création de la BNDJ prévoie que toutes les mises à jour de ce code doivent faire l'objet d'une traçabilité complète. En effet, il pourrait être déterminant de pouvoir analyser, *a posteriori*, si une extraction d'informations depuis l'un des traitements hébergés n'aurait pas été réalisée alors qu'un code n'était pas à jour ou dont le cas d'une mise à jour tardive. Il pourrait y avoir là une cause de nullité[1936].

1133. La continuité de la traçabilité des accès. – La journalisation des actions[1937] auxquelles les utilisateurs procèderaient sur les informations des différents traitements judiciaires hébergés au sein de la BNDJ serait différente de la traçabilité des accès[1938]. Cette dernière a vocation d'identifier un utilisateur. Le rapprochement de ces deux traçabilités assurerait une journalisation complète puisqu'il permettrait d'imputer

[1934] *Op. cit.* p.35. Sur les effets de la requalification judiciaire sur le TAJ, v. notamment BUISSON Jacques*, Preuve – Moyens de la preuve*, Dalloz Répertoire de droit pénal et de procédure pénale, Octobre 2019, chapitre 1, al.72.
[1935] V. *supra* n°663.
[1936] Sur le régime des nullités, v. *supra* n°856.
[1937] Modifications dont celles du code, saisies de nouvelles données ou effacements.
[1938] V. *supra* n°1124. Elle a vocation à identifier les connexions (utilisateur, horaire, adresse IP de connexion).

nominativement les opérations à une personne. L'ensemble de ces deux traçabilités reposerait sur ce que les informaticiens appellent un « système de logs[1939] ». Ceux-ci existent depuis longtemps mais prennent aujourd'hui une importance cruciale avec la cybersécurité puisqu'ils sont une source essentielle d'informations[1940].

1134. Le cadre légal de la traçabilité. – Deux journalisations doivent être distinguées. Celle qui serait créée par la BNDJ[1941] et visualisée sur l'illustration n°4[1942], et la traçabilité liée au fonctionnement des traitements judiciaires hébergés au sein de la BNDJ. En effet, le cadre légal de la journalisation créé par la BNDJ serait nouveau et devrait donc être entièrement créé. Certains fichiers de police, pour leur part, comportent des dispositions déjà existantes qui, par voie de conséquence, devraient être modifiées pour pouvoir s'imbriquer avec cette traçabilité qui serait introduite au travers de la BNDJ.

1135. Le nouveau cadre légal introduit par la création de la BNDJ. – Actuellement, des dispositions inhérentes à la traçabilité des actions existent pour les traitements de données judiciaires[1943]. Or, cette traçabilité génère évidemment la collecte de données personnelles pour tous les agents, militaires et autre personnel qui interviennent sur les fichiers de police[1944]. Ces utilisateurs sont, pour l'heure, les oubliés des règles qui s'appliquent en matière de droits liés aux données personnelles puisqu'à aucun moment, les dispositions des différents traitements sont claires par rapport aux données nominatives de traçabilité. Tout au plus, il existe un traitement de données automatisé s'intéressant à la gestion des accès au casier judiciaire[1945], mais celui-ci se borne à créer un historique des accès physiques aux locaux, notamment informatiques et techniques, du service du Casier judicaire.

[1939] Industrie et Technologies, *A Elancourt, Thales scrute 3 milliards d'événements de sécurité par jour*, Industrie et Technologies, 11 mars 2016. Entretien avec Thomas SAINTIN, responsable coordination technique au sein du CSOC de Thales : « Un système de log management permet d'abord de collecter tous les événements de sécurité. Un événement de sécurité peut être une simple connexion à un poste de travail ou la détection d'un virus sur un ordinateur […]. »

[1940] ROUSSEL Bruno, *Traitements de données à caractère personnel pour la cybersécurité : du difficile équilibre entre efficacité et respect des droits des salariés*, Lamy, Droit de l'immatériel, octobre 2018.

[1941] V. *supra* n°1087.

[1942] V. p. 35.

[1943] V. par ex. : le TAJ (C. pr. pén. art. R40-30), le fichier judiciaire national automatisé des auteurs d'infractions sexuelles ou violentes (C. pr. pén. R53-8-34), le fichier judiciaire national automatisé des auteurs d'infractions terroristes (C. pr. pén. R50-63).

[1944] *Ibid.* ROUSSEL Bruno, *Traitements de données à caractère personnel pour la cybersécurité.*

[1945] Arrêté du 22 février 2011 relatif à un traitement automatisé de données à caractère personnel aux fins de gestion des accès au casier judiciaire national

1136. La création de la BNDJ, qui viendrait considérablement renforcer la journalisation à la fois des accès et des actions sur les informations, devrait être l'occasion d'améliorer cette situation. Le chapitre deux, de la proposition de loi visant à améliorer l'efficacité et à renforcer les garanties des traitements de données en procédure pénale, dédié à la BNDJ, explicite que « les consultations ainsi que toutes les actions réalisées sur les données, font l'objet d'un enregistrement permettant une traçabilité complète. Les modalités de cette traçabilité sont précisées par décret[1946] ». Ce dernier apporte une double réponse à la nécessaire régularisation de la situation qui vient d'être dénoncée à l'égard des utilisateurs des traitements de données judiciaire. En premier lieu, le principe de la traçabilité complète ainsi que la liste des informations collectées au titre de la journalisation sont clairement explicités[1947]. En second lieu, l'exercice des droits liés aux traitements de données à caractère personnel par les utilisateurs est prévu. Le rôle du contrôleur de la BNDJ s'impose naturellement pour recevoir et traiter les demandes correspondantes[1948].

1137. Le constat du cadre légal des traitements judiciaires existants. – Comme cela vient d'être dit, il existe actuellement des dispositions qui prévoient la traçabilité pour les traitements de données judiciaires existants. Pour la quasi-totalité des traitements[1949] une journalisation des consultations est explicitement prévue. Ces dispositions rejoignent ici le critère technique d'auditabilité énoncé par le référentiel DICA des normes ISO

[1946] Annexe 2, proposition de loi, article 10, nouvel art. 230-51.
[1947] Annexe 4, projet de décret pris en application des dispositions relatives à la base nationale des données judiciaires, article 1, nouvel art. R40-58 : « En application de l'article 230-51, toutes les données de traçabilité d'utilisation de la base nationale des données judiciaires sont conservées pendant une durée de trois ans. Elles permettent l'identification de la personne ayant procédé à l'utilisation, la date et l'heure, ainsi que l'intégralité des opérations réalisées.
La personne qualifiée et les membres du comité prévus à l'article 230-52 ont un accès complet et permanent aux informations de traçabilité.
Ces informations, préalablement anonymisées, peuvent donner lieu à des exploitations statistiques. »
Nouvel art. R40-59 : « La base nationale des données judiciaires stocke et enregistre les catégories de données à caractère personnel et informations suivantes :
[…]
2° les données et informations de traçabilité en application de l'article R40-58 :
- identité (nom, prénom, identifiant, le cas échéant numéro de matricule) ;
- service, unité ou structure auquel appartient la personne ;
- adresse IP de connexion ;
- date, heure et durée de la connexion ;
- nature des opérations effectuées. »
[1948] *Ibid,* annexe 4, nouvel art. R40-62, deuxième alinéa : « Pour la catégorie des personnes prévue au 2° de l'article R40-59 [les personnes procédant à des opérations sur les informations de la BNDJ], les droits d'accès et de rectification s'exercent auprès de la personnalité prévue à l'article 230-52. »
Pour le contrôleur prévu à l'article 230-52 : v. *supra* n°1101.
[1949] Les exceptions notables qui peuvent être relevées sont le fichier des empreintes digitales et les fichiers Schengen. Selon le rapport Batho/Benisti (*op. cit.* p.35), le fichier des personnes recherchées comporte également des lacunes importantes en matière de traçabilité des données consultées (v. p. 95 du rapport).

2700x[1950]. Le cadre juridique prévu pour la journalisation de quelques traitements impose certains aspects techniques très précis. Une première illustration est fournie par le FIJAIS qui dispose que « le fichier conserve pendant une durée de trois ans les informations relatives aux enregistrements et interrogations dont il fait l'objet, en précisant la qualité de la personne ou autorité ayant procédé à l'opération[1951] ». Un second exemple, relatif aux données captées, précise que « toute opération relative au traitement fait l'objet d'un enregistrement comprenant l'identification de l'utilisateur, la date, l'heure et la nature de l'action. Ces informations sont conservées pendant une durée de cinq ans[1952] ».

1138. Conclusion du paragraphe §1 : le régime de la mise en œuvre opérationnelle de la BNDJ. – Le régime proposé pour la BNDJ serait une source importante d'amélioration du respect du droit des personnes en matière de données personnelles fortement sensibles. L'amélioration concernerait, bien sûr, les personnes concernées par les informations recueillies dans les fichiers, mais également les agents et les militaires qui manipulent ces informations et qui font actuellement l'objet d'une collecte de données sans que les traitements correspondants respectent les obligations en matière de données personnelles[1953]. Pour parvenir à cette amélioration, la BNDJ propose la mise en place d'un contrôle réel et effectif du respect des obligations légales s'imposant aux traitements judiciaires. Ce contrôle serait rendu possible grâce à un hébergement centralisé, en un même point et selon des modalités techniques identiques, de certains traitements judiciaires[1954]. Conjointement à la mise en place de ce contrôle s'appuyant sur un contrôleur et un comité, la BNDJ proposerait, techniquement, de mettre en place une traçabilité effective des actions et des accès. Cette traçabilité comporte deux objectifs. En premier lieu, il s'agit de permettre à l'instance de contrôle de disposer d'informations tangibles pour avoir la capacité d'exercer sa mission. En second lieu, cette traçabilité fournirait au juge des informations précises pour qu'il ait la capacité d'étudier la régularité des consultations et de l'exploitation des données. Une violation avérée de celles-ci pourrait être une source de nullité de l'extraction des données depuis le traitement judiciaire concerné.

[1950] V. *supra* n°1036.
[1951] C. pr. pén. art. R53-8-34 pour le fichier judiciaire national automatisé des auteurs d'infractions sexuelles ou violentes.
[1952] Décret n°2015-1700 du 18 décembre 2015 relatif à la mise en œuvre de traitements de données informatiques captées en application de l'article 706-102-1 du code de procédure pénale, art.6.
[1953] V. *supra* n°1135.
[1954] Sur la détermination des traitements susceptibles d'être hébergés par la BNDJ : v. *infra* n°1043.

1139. Le régime ainsi proposé pour de la BNDJ suppose que soient précisément énoncés des critères définissant les traitements judiciaires appelés à être hébergés au sein de celle-ci. Par voie de conséquence, les régimes des traitements actuels qui répondraient à ces critères devraient être adaptés.

§2. Le régime des traitements judiciaires dans le contexte de la BNDJ

1140. L'étude du régime en deux temps. – Après avoir énoncé une proposition de régime pour le fonctionnement général de la Base Nationale de Données Judiciaires, il est nécessaire d'étudier le régime des traitements judiciaires[1955] dans le contexte de la BNDJ. Deux catégories de traitements judiciaires doivent être distingués. En premier lieu, la BNDJ est conçue pour héberger des traitements judiciaires. Ce sont donc ces derniers, dont l'hébergement est proposé au sein de la BNDJ, qui constituent la première catégorie. Néanmoins, la technique permet d'aller plus loin. Ainsi, en second lieu, une autre catégorie rassemble les traitements judiciaires qui ne seraient pas hébergés au sein de la BNDJ car ne répondant pas au critère défini[1956], mais pour lesquels un lien informatique pour certaines données qu'ils contiennent est possible. Le régime de ces fichiers doit également être étudié.

1141. Or, pour étudier les régimes de ces deux catégories de traitements judiciaires, la façon de procéder est identique. Dans un premier temps, des critères sont nécessaires pour définir si un traitement judiciaire est susceptible d'être hébergé par la BNDJ, doit être lié à celle-ci ou, au contraire, doit rester totalement indépendant. Même si ces critères ont déjà été tacitement énoncés lors de la définition générale de la BNDJ[1957], ils doivent être reprécisés. Dans un second temps, lorsque les traitements judiciaires répondant à ces critères sont identifiés, il est nécessaire d'analyser les données qu'ils contiennent afin de déterminer celles qui doivent mises en commun et celles qui doivent rester séparées[1958]. Cette démarche en deux temps est celle qui devrait être utilisée dans le cas où un nouveau traitement judiciaire serait créé dans l'avenir[1959], afin de déterminer qu'elle doit être sa relation avec la BNDJ ainsi que le régime des données qu'il stockerait.

[1955] V. *supra* n°609.
[1956] V. *infra* n°1148.
[1957] V. *supra* n°1065.
[1958] V. *supra* n°1085.
[1959] La tendance actuelle est à la création fréquente de nouveaux fichiers de police, v. *supra* n°617.

1142. En conséquence, l'étude du régime des traitements hébergés au sein de la BNDJ *(I)* est distinguée de celle des traitements demeurant physiquement séparés, mais pour lesquels un lien informatique avec la BNDJ pourrait être envisagé *(II)*.

I – Le régime des traitements hébergés au sein de la BNDJ

1143. La nécessaire étude des données enregistrées. – L'hébergement commun d'un ensemble de traitements judiciaires par la BNDJ permettrait de regrouper certaines données qui sont communes à un ou plusieurs de ces fichiers. Pour atteindre cet objectif, il est nécessaire d'appliquer la démarche[1960] permettant de déterminer quels sont les traitements judiciaires appelés à bénéficier de cet hébergement centralisé *(A)*. Cette démarche conduit à étudier les données enregistrées dans ces traitements judiciaires et, par voie de conséquence, à proposer des évolutions du régime de ces données *(B)*.

A. La détermination des traitements judiciaires hébergés

1144. L'application de la démarche pour identifier les traitements à héberger dans la BNDJ. – Comme indiqué précédemment[1961], la démarche pour déterminer les traitements judiciaires qui devraient être hébergés dans la BNDJ, nécessite de préciser le critère que doivent respecter ces fichiers *(1)* puis, dans un second temps, d'analyser les données contenues afin de déterminer celles qui doivent être mises en commun et celles qui doivent rester cloisonnées *(2)*.

1. Le critère pour les traitements hébergés

1145. Le double intérêt du critère. – Ce critère a tacitement été évoqué lorsque le cadre général de la BNDJ a été présenté[1962]. Pour autant, il est nécessaire de le rappeler clairement car il est indispensable, d'une part pour identifier, parmi la multitude de traitements judiciaires actuels, ceux qui pourraient être hébergés dans la BNDJ et, d'autre part, pour l'avenir lorsque de nouveaux fichiers de police seront créés, savoir s'il serait pertinent de les ajouter à la BNDJ.

[1960] V. *supra* n°1141.
[1961] *Ibid.*
[1962] V. *supra* n°1065.

1146. Rappel sur la notion de traitement judiciaire[1963]. – Dans la présente étude, un traitement judiciaire désigne un traitement de données à caractère personnel mis en œuvre par l'Etat, et dont la consultation constitue une investigation numérique[1964]. De plus, pour être un traitement judiciaire, un accès direct doit être prévu pour les autorités judiciaires lors des enquêtes pénales. Cela signifie que les autorités judiciaires n'ont pas à utiliser une réquisition[1965] pour avoir accès aux informations numériques enregistrées dans le fichier concerné.

1147. Rappel sur l'objectif de la BNDJ. – Avec la proposition de création d'une BNDJ, il ne s'agit en aucun cas de proposer la création d'une base de données introduisant un fichage global et général des individus, notamment en consolidant les informations de traitements aux finalités totalement inconciliables[1966]. C'est pourquoi tous les fichiers à vocation de police administrative et de sécurité publique[1967], ne doivent pas être hébergés par la BNDJ.

1148. Le critère de la finalité. – Parmi la multitude de traitements judiciaires[1968], seuls les traitements judiciaires dont la finalité principale[1969] est de concourir à l'exercice de l'action pénale pourraient bénéficier d'un hébergement mutualisé. Les fichiers auxquels les enquêteurs ont directement accès lors d'une enquête pénale, mais dont la finalité principale n'est pas la constatation et la poursuite des infractions pénales[1970] ne devraient pas être hébergés par la BNDJ.

1149. L'identification des traitements judiciaires actuel qui pourraient être hébergés au sein de la BNDJ. – Dans ce contexte et en application du critère défini, il

---

[1963] V. *supra* n°614.
[1964] V. *supra* n°155.
[1965] V. *supra* n°372.
[1966] V. *supra* n°965.
[1967] Les principaux fichiers sont « gestion des sollicitations et des interventions » (v. *supra* n°708.), « enquêtes administratives liées à la sécurité publique (EASP) » (v. *supra* n°709.), « prévention des atteintes à la sécurité publique (PASP) » *(ibid.)* et « gestion de l'information et prévention des atteintes à la sécurité publique » *(ibid.)*.
[1968] V. *supra* n°615.
[1969] C'est-à-dire les fichiers dont la finalité s'inscrit dans un objectif « de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales ».
V. la Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes 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.
[1970] V. les traitements dont la finalité principale est administrative, comme, par exemple, les fichiers des cartes grises et des permis de conduire : v. *supra* n°697.

est possible d'identifier, parmi les fichiers actuels, ceux répondant à la finalité principale de constatation et de poursuite des infractions pénales. Tout d'abord, Cassiopée[1971] et le Traitement des Antécédents Judiciaires[1972] qui, respectivement, sont le support de la gestion des procédures sur l'ensemble du territoire et l'outil de travail des officiers de police judiciaire dans le quotidien de leurs enquêtes, seraient essentiels au fonctionnement de la BNDJ. Ensuite, le fichier des personnes recherchées[1973], le fichier automatisé des empreintes digitales[1974] et le fichier national automatisé des empreintes génétiques[1975], sont des traitements judiciaires dont la consultation est susceptible[1976] d'être au cœur des enquêtes pénales. Enfin, le fichier judiciaire national automatisé des auteurs d'infractions sexuelles ou violentes[1977] et le fichier judiciaire national automatisé des auteurs d'infractions terroristes[1978], relatifs à des individus à la dangerosité potentielle importante, entreraient parfaitement dans la nécessité d'être hébergés par la BNDJ.

1150. Une imbrication des dispositions proposées assurant la souplesse des modifications ultérieures. – Le chapitre deux, de la proposition de loi visant à améliorer l'efficacité et à renforcer les garanties des traitements de données en procédure pénale, dédié à la BNDJ, fait référence aux traitements hébergés en se limitant toutefois à en officialiser l'existence[1979]. La description de la liste est renvoyée au projet de décret d'application[1980]. Cette façon de procéder présenterait l'avantage d'apporter de la souplesse dans la modification ultérieure de la liste des traitements hébergés, afin d'anticiper l'ajout d'un nouveau traitement[1981].

[1971] V. *supra* n°623.
[1972] V. *supra* n°642.
[1973] V. *supra* n°655.
[1974] V. *supra* n°661.
[1975] *Ibid.*
[1976] Le régime pour la consultation de certains traitements judiciaires limite leur interrogation à certaines infractions. V. par ex. le fichier national automatisé des empreintes génétiques : C. pr. pén. art. 706-54 et 706-55.
[1977] V. *supra* n°667.
[1978] *Ibid.*
[1979] Annexe 2, proposition de loi, article 10, nouvel art. 230-47 : « Afin de faciliter la mise à jour et le contrôle des informations enregistrées dans les traitements automatisés de données à caractère personnel dont la liste est précisée par décret […]. »
[1980] Annexe 4, projet de décret pris en application des dispositions relatives à la base nationale des données judiciaires, article 1, nouvel art. 40-57.
[1981] La tendance actuelle est à la création fréquente de nouveaux fichiers - V. *supra* n°617.

1151. De plus, la proposition de loi intègre les ajustements nécessaires pour les dispositions des sept traitements appelés à être hébergés, qui s'inscrivent jusqu'ici dans une logique de dispersion de leur supervision[1982].

1152. Conclusion du sous-paragraphe 1 : les critères pour les traitements judiciaires hébergés. – Dès lors que les traitements judiciaires susceptibles d'être hébergés dans la BNDJ sont identifiés, la démarche se poursuit avec l'étude des données qu'ils contiennent afin de déterminer celles qui devraient mises en commun et celles qui devraient rester séparées

2. L'étude des données enregistrées dans les traitements hébergés

1153. La cartographie des données contenues. – Dès lors que la liste des traitements de données judiciaires appelés à être hébergés dans la BNDJ est établie, un travail indispensable consiste à réaliser une cartographie des données. Il s'agit, à partir des dispositions énonçant la liste des données collectées pour chaque traitement, de les recenser exhaustivement afin de pouvoir mettre en évidence leur redondance d'un fichier à un autre. Le résultat de ce recensement est présenté sous la forme d'un tableau en annexe 5. L'illustration n°6 (en page suivante) montre un extrait du tableau obtenu afin d'en expliquer le principe.

…/…

[1982] Annexe 2, proposition de loi, article 11, venant modifier l'art. 230-6 du C. pr. pén. relatif aux fichiers des antécédents.
Article 12, venant modifier l'art. 48-1 du C. pr. pén. relatif à Cassiopée.
Article 13, venant modifier l'art. 706-54 du C. pr. pén. relatif au fichier national automatisé des empreintes génétiques.
Article 14, venant modifier l'art. 706-53-1 du C. pr. pén. relatif au fichier judiciaire national automatisé des auteurs d'infractions sexuelles ou violentes.
Article 15, venant modifier l'art. 706-25-3 du C. pr. pén. relatif au fichier judiciaire national automatisé des auteurs d'infractions terroristes.

Annexe 4, projet de décret pris en application des dispositions relatives à la base nationale des données judiciaires, article 4 venant modifier le décret n°2010-569 du 28 mai 2010 relatif au fichier des personnes recherchées.
Article 5 venant modifier le décret n°87-249 du 8 avril 1987 relatif au fichier automatisé des empreintes digitales.

Catégorie permettant de classer les données

	Cassiopée	Traitement d'antécédents judiciaires	Fichier des personnes recherchées
III	Faits - description	Faits - description	
	Récidive		
		Objets de l'enquête	
	Code nat inf. NATINF		
			Motifs de la recherche
			Actes admin. ou judi.
	Lieux infraction	Lieux infraction	
	Date infraction	Date infraction	
		Mode opératoire	
		Photos objets	
		Description objets	

Illustration n°6 : extrait de la cartographie des données des traitements hébergés

1154. L'identification de six catégories de données. – Chaque donnée fait l'objet d'une ligne unique dans le tableau. Il est ainsi possible de visualiser immédiatement la redondance d'une même information dans les différents fichiers hébergés par la BNDJ. Cette cartographie permet alors d'établir un classement des données qui sont enregistrées dans les sept traitements. Six catégories se dégagent. Lorsque cela est nécessaire[1983], des sous-catégories introduisent un degré de granularité plus efficace[1984].

1155. En premier lieu, une catégorie est constituée par les données d'identification[1985] (numérotées « I »), au sein desquelles il convient de distinguer celles des personnes physiques et des personnes morales. Cette deuxième sous-catégorie n'est utile que pour

[1983] Les données d'identification (v. *infra* n°1155.), celles relatives au suivi judiciaire de la procédure (v. *infra* n°1158.) et les informations concernant les intervenants dans la procédure (v. *infra* n°1160.).
[1984] Ces six catégories ainsi que les sous-catégories sont matérialisées dans la colonne de gauche du tableau (v. illustration n°6) et elles sont rappelées sous forme de légende en dernière page de l'annexe 5.
[1985] V. par ex. le fichier des personnes recherchées (Décret n°2010-569 du 28 mai 2010 relatif au fichier des personnes recherchées, art. 3 : « Pour chaque personne inscrite dans le traitement, donnent lieu à enregistrement les données à caractère personnel et informations suivantes :
1° L'état civil (nom, prénom[s], date et lieu de naissance, filiation), l'alias, le sexe, la nationalité ; […] ») ou le fichier automatisé des empreintes digitales (Décret n°87-249 du 8 avril 1987 relatif au fichier automatisé des empreintes digitales géré par le ministère de l'intérieur, art. 4 : « Les empreintes digitales et palmaires enregistrées sont accompagnées des informations suivantes :
1° Le sexe de la personne et, lorsqu'ils sont connus, ses noms, prénoms, date et lieu de naissance et éléments de filiation ; […] »).

Cassiopée[1986] et le TAJ[1987] car les autres traitements ne concernent que des personnes physiques.

1156. En deuxième lieu, les éléments judiciaires pour les antécédents (numérotés « II ») constituent une autre catégorie. Il ne s'agit pas uniquement ici des antécédents au sens strict du terme[1988]. Toutes les informations associées aux antécédents[1989] sont disponibles pour les procédures à venir.

1157. En troisième lieu, les éléments factuels de la procédure en cours (numérotés « III ») contiennent les éléments matériels des faits qui sont à l'origine de l'ouverture d'une enquête[1990].

1158. En quatrième lieu, on peut regrouper dans une catégorie « IV » le suivi judiciaire de la procédure en cours. Il convient ici de distinguer les informations détaillées[1991], des éléments généraux que sont la référence de la procédure et la situation dans la procédure[1992]. Ces deux données joueraient un rôle déterminant dans le fonctionnement de la BNDJ puisqu'elles permettraient de coordonner, d'un point de vue numérique, l'enregistrement des informations dans les différents traitements[1993].

[1986] C. pr. pén. art. R15-33-66-6 : « […] identification : dénomination/raison sociale, situation juridique, enseigne, sigle, numéro SIREN ou SIRET, forme juridique, numéro au registre du commerce et des sociétés, date et lieu de la création de la société ; […] siège social ou établissement, adresse, code postal, libellé ville associé au code postal, Cedex, pays ; […] »

[1987] C. pr. pén. art. R40-26 : « […] b) Personnes morales : raison sociale, enseigne commerciale, sigle ; forme juridique ; numéro d'inscription au registre du commerce et des sociétés ; lieu du siège social ; numéro SIREN, SIRET ; secteur d'activité ; adresses ; […] ».

[1988] Comme par ex. dans Cassiopée, C. pr. pén. art. R15-33-66-6 : « […] 2° Concernant les infractions, condamnations ou mesures de sûreté : -situation judiciaire des personnes au cours de la procédure, antécédents relatifs aux condamnations de l'auteur des faits ; […] ».

[1989] Par ex. le signalement (Ex. le fichier des personnes recherchées : Décret n°2010-569 du 28 mai 2010 relatif au fichier des personnes recherchées, art. 3) dans le ou les photographies (Ex. le fichier automatisé des empreintes digitales : Décret n°87-249 du 8 avril 1987 relatif au fichier automatisé des empreintes digitales géré par le ministère de l'intérieur, art. 4 : « […] 5° Les clichés anthropométriques ; […] »).

[1990] Dans le cas, par ex., du fichier national automatisé des empreintes génétiques, il s'agit de la « nature de l'affaire » (C. pr. pén. art. R53-11).

[1991] Sous-catégorie « IV-B » qui regroupe les informations telles que la situation pénale de l'individu fiché (v. par ex. le FIJAIS, C. pr. pén. art. R53-8-7 : « […] 2° Informations relatives à la ou aux décisions ayant donné lieu à l'enregistrement : -nature et date de la décision ; -juridiction ayant prononcé la décision ; […] -date d'exécution ou de fin d'exécution de la peine ou de la mesure ; -le cas échéant, dates de mise sous écrou et de libération ; […] . »

[1992] V. par ex. le fichier national automatisé des empreintes génétiques, C. pr. pén. art. R53-11 : « 1° Le numéro de la procédure dans le cadre de laquelle l'enregistrement au fichier est demandé ; […]. »

[1993] V. *infra* n°1174.

1159. En cinquième lieu, on distinguera les données spécifiques au cœur des traitements, numérotées « V », comme les empreintes[1994], les informations accompagnant les données génétiques[1995], ou encore la conduite à tenir pour les personnes recherchées[1996].

1160. Enfin, en sixième et dernier lieu, les informations relatives aux intervenants dans la procédure (numérotées « VI »), concernent tous les agents (les policiers ou encore les fonctionnaires du ministère de la justice) et les militaires qui utilisent les différents traitements[1997]. Cette catégorie de données correspond au traitement mis en œuvre pour la traçabilité de tous les accès et de toutes les actions que les utilisateurs habilités réalisent sur les données[1998]. On ajoute au sein de cette catégorie les informations des avocats[1999], qui sont une spécificité de Cassiopée[2000]. Les avocats ne sont pas des utilisateurs directs des traitements, mais ils sont des intervenants dans la procédure. A ce titre les données qui les concernent doivent être distinguées de celles des justiciables. En assimilant leurs données nominatives à celles des intervenants dans la procédure, leurs informations se retrouvent donc protégées.

1161. Conclusion du sous-paragraphe A : la détermination des traitements judiciaires hébergés. – Ce sont sept fichiers, parmi la multitude de traitements judiciaires[2001] existants, qui remplissent la double condition de constituer une investigation numérique en procédure pénale[2002], et dont la finalité est directement en lien avec l'objectif « de prévention et de détection des infractions pénales, d'enquêtes et de

[1994] Fichier automatisé des empreintes digitales (Décret n°87-249 du 8 avril 1987 relatif au fichier automatisé des empreintes digitales géré par le ministère de l'intérieur, art. 3) et fichier national automatisé des empreintes génétiques (C. pr. pén. art. R53-10).
[1995] Comme par exemple « le nom de la personne physique ou morale habilitée ayant réalisé l'analyse » (C. pr. pén. R53-11).
[1996] Décret n°2010-569 du 28 mai 2010 relatif au fichier des personnes recherchées, art. 3, 4°.
[1997] V. par ex. le fchier automatisé des empreintes digitales (Décret n°87-249 du 8 avril 1987 relatif au fichier automatisé des empreintes digitales géré par le ministère de l'intérieur, art. 4 : « […] Les traces d'empreintes enregistrées sont accompagnées des informations suivantes : […] 2° Le service ayant procédé au relevé des traces ; […]) ou le fichier national automatisé des empreintes génétiques (C. pr. pén. art. R53-11 : « […] 2° L'autorité judiciaire ou l'officier de police judiciaire ayant demandé l'enregistrement au fichier ; […]. »
[1998] V. *supra* n°1133. Ces données sont regroupées sans la sous-catégorie « VI-B ».
[1999] Les données relatives aux avocats constituent la sous-catégorie « VI-A ».
[2000] C. pr. pén. art. R15-33-66-6 : « […] e) Concernant les avocats : -nom de naissance ou d'usage et prénoms ; -numéro d'affiliation à la Caisse nationale des barreaux français ; -nom du barreau auquel l'avocat est rattaché, adresse postale du cabinet, adresse interne : numéro de toque, référence ou adresse locale dans la juridiction, adresse de messagerie électronique, numéro de téléphone et numéro de télécopie du cabinet ; […]. »
[2001] Sur la notion de traitements judiciaires au sens de la présente étude, v. *supra* n°968.
[2002] Sur la notion d'investigation numérique en procédure pénale, v. *supra* n°194.

poursuites en la matière ou d'exécution de sanctions pénales[2003] ». Une cartographie des données enregistrées dans ces sept traitements, permet de répartir celles-ci en différentes catégories.

1162. Cette répartition en catégorie est un prérequis indispensable à l'étude de l'évolution du régime des sept traitements dont l'hébergement au sein de la BNDJ est proposé.

B. L'évolution du régime des données enregistrées dans les traitements hébergés

1163. La distinction de deux propositions de modifications. – En premier lieu, l'évolution du régime des traitements judiciaires dont l'hébergement dans la BNDJ est étudiée au travers de la légalisation de la mise en commun de certaines données *(1)*. En second lieu, la proposition de créer une BNDJ comporte un ensemble d'améliorations du régime des données enregistrées dans les sept traitements judiciaires *(2)*.

1. L'évolution du régime par la mise en commun de certaines données

1164. L'adéquation des catégories et des dispositions proposées pour la BNDJ. – La répartition en catégories de l'ensemble des informations contenues dans les traitements judiciaires appelés à être hébergés par la BNDJ[2004], permet d'étudier la mise en œuvre du cadre légal général précédemment proposé[2005]. En effet, ce dernier a, notamment, pour objectif de proposer la création d'une mise à jour automatique de données communes à un ou plusieurs traitements, tandis que celles constituant le cœur de chaque fichier de police[2006] resteraient cloisonnées.

1165. L'adéquation des catégories avec l'interconnexion. – Des règles pour autoriser les interconnexions entre les traitements judiciaires dont l'hébergement est proposé dans la BNDJ sont prévues dans le cadre général qui a été défini pour cette entité[2007]. C'est cette interconnexion qui permettrait les mises à jour automatique des données communes. Il est nécessaire de prévoir des adaptations afin de modifier tous les articles qui interdisent

[2003] 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.
[2004] V. *supra* n°1153.
[2005] V. *supra* n°1068.
[2006] Celles de la catégorie « V ». V. *supra* n°1159.
[2007] V. *supra* n°1096.

l'interconnexion au sein des sept traitements concernés par la mise en relation de certaines données[2008].

1166. L'adéquation des catégories avec le maintien du cloisonnement pour le cœur des traitements judiciaires. – Les utilisateurs ne pourraient accéder aux données constituant le cœur de chaque fichier de police que dans des conditions strictement encadrées[2009]. L'analyse de la cartographie[2010] conduit à proposer la mise en commun des données des catégories « I, II, III et IV » pour l'ensemble des traitements hébergés. Ces données bénéficieraient ainsi des mises à jour automatiques pour tous les traitements hébergés. Parmi ces données, deux types d'informations sont distinguées : les informations communes à tous les traitements comme l'identité, et celles qui ne sont présentes que dans certains fichiers, mais pas tous[2011]. Le fonctionnement de la BNDJ avec la mise en œuvre de ces catégories de données est matérialisé avec l'illustration n°7 (voir en page suivante).

…/…

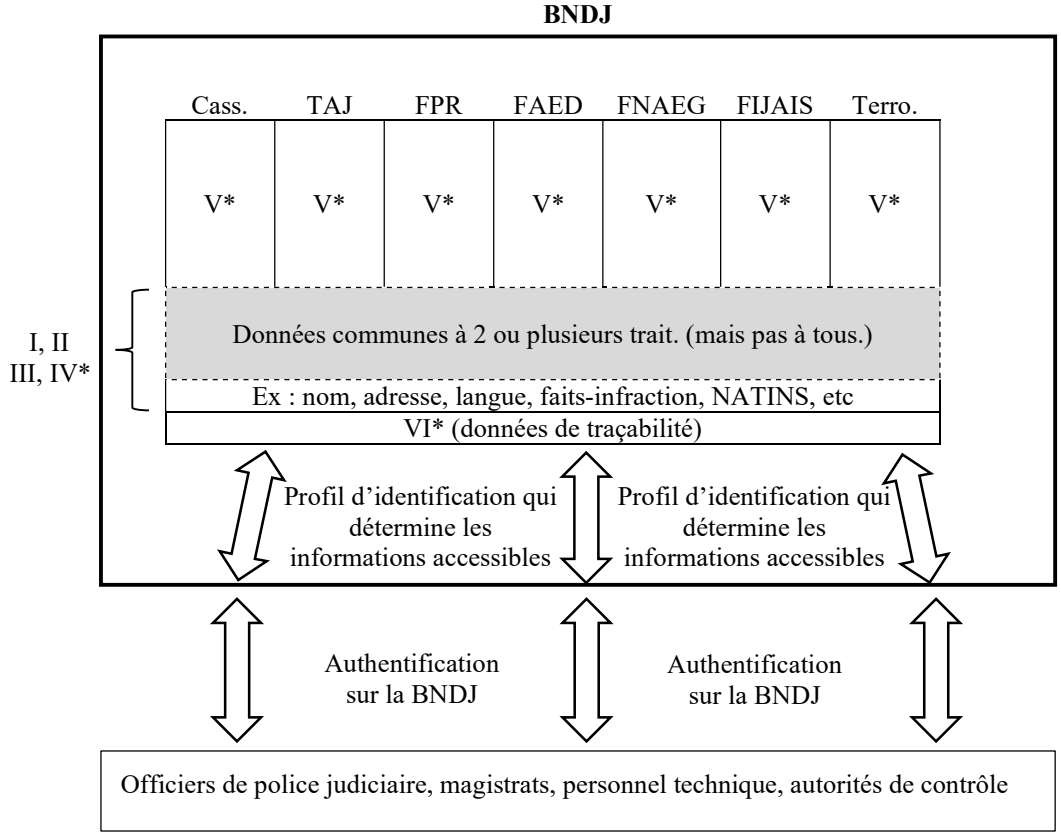
[2008] Annexe 2, proposition de loi, article 14, venant modifier l'art. 706-53-11 du C. pr. pén. relatif au fichier judiciaire national automatisé des auteurs d'infractions sexuelles ou violentes.
Article 15, venant modifier l'art. 706-25-13 du C. pr. pén. relatif au fichier judiciaire national automatisé des auteurs d'infractions terroristes.
Article 16, venant modifier l'art. 777-3 du C. pr. pén. relatif au Casier judiciaire.

Annexe 4, projet de décret pris en application des dispositions relatives à la base nationale des données judiciaires, article 3 venant modifier l'art. R15-33-66-12 du C. pr. pén. relatif à Cassiopée.
Article 5 venant modifier le décret n°87-249 du 8 avril 1987 relatif au fichier automatisé des empreintes digitales.
Article 6 venant modifier l'art. R53-19 du C. pr. pén. relatif au fichier national automatisé des empreintes génétiques.

[2009] V. *supra* n°1123.

[2010] V. annexe 5. V. *supra* n°1153.

[2011] Par ex., les données relatives aux condamnations et à la peine prononcée ne sont présentes que dans Cassiopée (C. pr. pén. R15-33-66-6 : « […] peine prononcée, libellé de la peine et mesure, motifs, obligations. […]), le FIJAIS (C. pr. pén. R53-8-7) et le fichier judiciaire national automatisé des auteurs d'infractions terroristes (C. pr. pén. art. R50-36).



(*)
I : Données d'identification
II : Eléments judiciaires pour les antécédents
III : Les éléments factuels de la procédure
IV : Le suivi judiciaire de la procédure
V : Données spécifiques aux traitements particuliers
VI : Informations relatives aux intervenants dans la procédure

Illustration n°7 : architecture de la BNDJ

1167. Le double objectif de la proposition de création de la BNDJ. – La proposition de créer un hébergement regroupé de sept traitements judiciaires[2012] a pour objectif premier de mettre en commun les données transversales à ces différents fichiers, sans porter atteinte au principe de séparation des informations constituant le cœur des traitements judiciaires[2013]. Cet objectif permettrait d'améliorer, à la fois, la qualité des données contenues dans les fichiers de police[2014], et la mise en œuvre de contrôles effectifs sur l'utilisation et la mise à jour des informations enregistrées[2015], comme le

[2012] Sur la liste des sept traitements judiciaires, v. *supra* n°1149.
[2013] V. *supra* n°1164.
[2014] Sur les problèmes actuels de fiabilité des données actuellement enregistrées dans les traitements judiciaires, v. *supra* n°1047.
[2015] Sur l'incompatibilité entre la mise en œuvre effective des contrôles prévus pour les traitements judiciaires et l'éparpillement de ces derniers, v. *supra* n°1025.

cadre général proposé pour la BNDJ le prévoit[2016]. Il est nécessaire de proposer des modifications pour les septs traitements dont l'hébergement au sein de la BNDJ est proposé permettant de concrétiser les contrôles prévus[2017].

1168. Un deuxième objectif de la BNDJ, est d'énoncer, au travers de la proposition de loi « visant à améliorer l'efficacité et à renforcer les garanties des traitements de données en procédure pénale[2018] », des améliorations générales du régime des données enregistrées dans les fichiers de police.

2. Les propositions d'améliorations transversales aux régimes des données

1169. La nécessité d'homogénéiser et d'améliorer la cohérence des données au sein des différents traitements. – L'analyse de la cartographie des sept traitements judiciaires dont l'hébergement est proposé au sein de la BNDJ révèle que de nombreuses incohérences existent dans les données collectées dans ces fichiers. Ils sont créés à des périodes très différentes[2019], ce qui peut expliquer que le législateur n'utilise pas forcément le même vocabulaire au fil des années.

[2016] V. *supra* n°1104.

[2017] Annexe 2, proposition de loi, article 11, venant modifier l'art. 230-8 du C. pr. pén. relatif au fichier des antécédents.
Article 13, venant modifier l'art. 706-54 du C. pr. pén. relatif au fichier national automatisé des empreintes génétiques.
Article 14, venant modifier l'art. 706-53-10 du C. pr. pén. relatif au fichier judiciaire national automatisé des auteurs d'infractions sexuelles ou violentes.
Article 15, venant modifier l'art. 706-25-12 du C. pr. pén. relatif au fichier judiciaire national automatisé des auteurs d'infractions terroristes.

Annexe 4, projet de décret pris en application des dispositions relatives à la base nationale des données judiciaires, article 2 venant modifier l'art. R40-31 du C. pr. pén. relatif au fichier des antécédents.
Article 3 venant modifier l'art. R15-33-66-5 du C. pr. pén. relatif à Cassiopée.
Article 4 venant modifier le décret n°2010-569 du 28 mai 2010 relatif au fichier des personnes recherchées.
Article 5 venant modifier le décret n°87-249 du 8 avril 1987 relatif au fichier automatisé des empreintes digitales.
Article 6 venant modifier l'art. R53-13-5 du C. pr. pén. relatif au fichier national automatisé des empreintes génétiques.
Article 7 venant modifier l'art. R53-8-31 du C. pr. pén. relatif au fichier judiciaire national automatisé des auteurs d'infractions sexuelles ou violentes.
Article 8 venant modifier l'art. R50-59 du C. pr. pén. relatif au fichier judiciaire national automatisé des auteurs d'infractions terroristes.

[2018] En annexe 2 des présentes.

[2019] Le fichier automatisé des empreintes digitales a été officialisé par le décret n°87-249 du 8 avril 1987 relatif au fichier automatisé des empreintes digitales géré par le ministère de l'intérieur. Le fichier judicaire national automatisé des auteurs d'infractions terroristes a été créé par la loi n°2015-912 du 24 juillet 2015 relative au renseignement.
THOMAS-TAILLANDIER Delphine, *Le nouveau fichier national des auteurs d'infractions terroristes*, Dalloz AJ pénal 2015.

1170. Des propositions d'améliorations. – C'est pourquoi, un projet d'amélioration de la cartographie précédemment réalisée[2020] est proposé. Celui-ci comporte l'ensemble des améliorations qui sont décrites dans la suite des présentes. Ainsi, l'annexe 6 reprend la cartographie des données contenues dans les traitements judiciaires, en y intégrant ces améliorations. Ce projet de cartographie se concrétise au travers de modifications des dispositions existantes pour les sept traitements appelés à être hébergés dans la BNDJ. Ces dispositions sont toutes de la compétence du pouvoir règlementaire car le descriptif des informations déclarées pour l'ensemble des fichiers de police est toujours dans la partie règlementaire du Code de procédure pénale ou dans des décrets[2021]. Les modifications proposées sont donc intégrées au « projet de décret pris en application des dispositions relatives à la base nationale des données judiciaires[2022] ». En effet, de telles adaptations sont associées à la création de la BNDJ. Par voie de conséquence, le fait de regrouper toutes les propositions de dispositions liées à la BNDJ dans un même texte est une source de cohérence.

1171. Les modifications liées à l'intégration d'un code transversal à tous les traitements judiciaires appelés à être hébergés dans la BNDJ *(a)* sont distinguées de diverses adaptations destinées à homogénéiser et améliorer la cohérence des informations enregistrées dans ces fichiers *(b)*.

a. L'amélioration par l'introduction de codes transversaux

1172. Un traitement de référence. – L'analyse de la cartographie actuelle[2023] démontre que Cassiopée devrait être pris comme la référence pour le socle de données générales et, par là-même, devrait servir de modèle pour homogénéiser les informations des autres fichiers. Au demeurant, ce rôle de Cassiopée serait en adéquation avec le respect des droits des personnes fichées car il s'agit d'un traitement directement contrôlé par les

[2020] V. annexe 5. V. *supra* n°1047.
[2021] *Op. cit.* pour le fichier automatisé des empreintes digitales. Par ex. le traitement d'antécédents judiciaires (C. pr. pén. art. R40-23 et s.), le fichier des personnes recherchées (Décret n°2010-569 du 28 mai 2010 relatif au fichier des personnes recherchées).
[2022] V. annexe 4.
[2023] V. annexe 5, cartographie issue des dispositions actuelles des traitements appelés à être hébergés par la BNDJ.

autorités judiciaires[2024]. Le positionnement comme référence pour la mise à jour des données dans d'autres fichiers de police est déjà prévu[2025].

1173. Une incohérence devrait toutefois être rectifiée puisque le numéro de procédure géré par Cassiopée, servant de base pour l'identification unique au niveau national d'un dossier pénal, ne fait pas explicitement partie des données déclarées pour ce traitement alors qu'il l'y ait fait référence dans d'autres[2026]. Ainsi, le projet de « décret pris en application des dispositions relatives à la base nationale des données judiciaires[2027] » propose de concrétiser l'officialisation du numéro de procédure dans tous les traitements appelés à être hébergés par la BNDJ[2028], au travers d'une donnée intitulée « référence procédure ». Cette donnée est indirectement nominative puisqu'une recherche sur cette référence au sein de l'un des traitements de données serait susceptible de révéler toutes les personnes mises en cause ou condamnées, ainsi que les témoins et les victimes, désignés dans ce dossier. Il y a là une difficulté qui doit faire l'objet d'une amélioration[2029]. Néanmoins, grâce à cette proposition d'intégrer le même numéro de procédure dans tous les fichiers, l'optimisation de la chaîne pénale serait accrue. En effet, la saisie d'informations nominatives dans Cassiopée s'en trouverait accélérée dans la mesure où toutes les données d'identité auraient déjà été saisies, notamment par les enquêteurs lors des auditions ou des gardes à vue. De plus, une vérification lors de l'ouverture du dossier dans Cassiopée serait l'occasion de contrôler les informations précédemment saisies, améliorant ainsi la fiabilité des données contenues dans la BNDJ[2030].

[2024] Sur la nécessité du contrôle du juge sur les informations contenues dans les traitements judiciaires, v. BEGRANGER Gérald, *Le contrôle des fichiers de police par les juges*, Dalloz, AJ pénal 2014. p.176.

[2025] Sur les mises à jour automatiques de Cassiopée vers d'autres fichiers de police, v. *supra* n°1057. BEYNEL Jean-François et CASAS Didier, *Chantiers de la justice – Transformation numérique*, Ministère de la Justice, 2018 : « Mise à disposition de nombreuses applications expérimentales (les échanges inter-applicatifs entre le Casier Judiciaire et Cassiopée […]. »

[2026] Dans le fichier automatisé des empreintes digitales (Décret n°87-249 du 8 avril 1987 relatif au fichier automatisé des empreintes digitales géré par le ministère de l'intérieur, art. 4 : « […] la référence de la procédure. […] ») et dans le fichier national automatisé des empreintes génétiques (C. pr. pén. art. R53-11 : « […] 1° Le numéro de la procédure dans le cadre de laquelle l'enregistrement au fichier est demandé ; […] ».

[2027] Annexe 4.

[2028] Annexe 4, projet de décret pris en application des dispositions relatives à la base nationale des données judiciaires, articles 11, 12, 13, 16 et 17.

[2029] V. *infra* n°1174.

[2030] Et par voie de conséquence dans tous les traitements judiciaires dont l'hébergement regroupé est proposé, ce qui contribuerait à améliorer l'une des difficultés actuelles que constitue le manque de fiabilité des informations enregistrées : v. *supra* n°1013.

1174. L'intégration d'un code relatif au motif d'inscription dans les fichiers de police. – L'amélioration de la cohérence générale des données repose, en premier lieu, sur la référence d'une procédure gérée par Cassiopée qui devrait devenir un élément commun à l'ensemble des traitements judiciaires appelés à être hébergés par la BNDJ. En second lieu, cette amélioration comporte également la proposition de créer un code permettant de catégoriser les données personnelles présentes dans les traitements de données hébergés dans la BNDJ[2031], comme expliqué précédemment[2032]. Ce code serait une avancée notable pour améliorer le respect des droits des personnes dont les données sont collectées, puisque seules les données des personnes mises en cause ou précédemment condamnées pourraient être consultées ou extraites lors de l'interrogation d'un traitement dans le cadre d'une investigation[2033]. L'interdiction qui en découle d'extraire des données relatives aux victimes ou aux témoins lors de ces consultations doit être intégrée dans les propositions de modifications des dispositions des sept traitements pour lesquels l'hébergement au sein de la BNDJ est proposé[2034].

1175. De plus, il est nécessaire de modifier la cartographie actuelle des informations collectées pour ces sept traitements, afin de donner une existence légale à ce code. Ainsi, dans le projet d'amélioration de la cartographie des données[2035], ce code est introduit sous le nom « NATINS » qui s'inspire du code « NATINF », présent dans Cassiopée[2036]. « NATINS » est l'acronyme de « nature de l'inscription ». Le projet de décret d'application de la BNDJ propose de modifier les dispositions existantes de tous les

---

[2031] V. *supra* n°1127. Quatre catégories sont proposées : les personnes mises en cause, condamnées ou recherchées – Les témoins – Les victimes – Les avocats, les agents ou militaires intervenants sur les données des traitements hébergés par la BNDJ.

[2032] V. le cadre général du régime de la BNDJ : v. *supra* n°1126.

[2033] V. *supra* n°1130.

[2034] Annexe 2, proposition de loi, article 13 venant modifier l'art. 706-54 du C. pr. pén. relatif au fichier national automatisé des empreintes génétiques : « En aucun cas ce rapprochement ne peut conduire à l'extraction d'informations relatives aux autres catégories de personnes. »

Annexe 4, projet de décret pris en application des dispositions relatives à la base nationale des données judiciaires, article 7 venant modifier l'art. R53-8-23 du C. pr. pén. relatif au fichier judiciaire national automatisé des auteurs d'infractions sexuelles ou violentes : « Cette interrogation n'est opérée que sur la catégorie des personnes mises en cause, condamnées ou recherchées […] ».
Article 8 venant modifier l'art. R50-51 du C. pr. pén. relatif au fichier judiciaire national automatisé des auteurs d'infractions terroristes : *idem*.

[2035] Annexe 6, projet de cartographie améliorée.

[2036] C. pr. pén. art. R.15-33-66-6, 2° avant dernier alinéa : « […] Code de nature d'infraction NATINF […] ».

traitements appelés à être hébergés pour y intégrer le NATINS[2037]. Ce code est matérialisé dans l'illustration n°7 au sein des données communes à tous les traitements[2038].

1176. Le principe de Cassiopée comme source d'affectation du NATINS. – L'attribution des trois premiers codes à une personne faisant l'objet d'une procédure judiciaire[2039], ainsi que sa mise à jour ultérieure au fil de l'évolution du dossier, devrait directement découler de la donnée « situation judiciaire dans la procédure » prévue au sein de Cassiopée[2040]. Comme précédemment expliqué, il est essentiel de savoir à quel titre une personne fait l'objet d'une saisie d'informations personnelles dans l'un ou plusieurs des traitements judiciaires. Cassiopée est le traitement de référence et devrait donc être à l'origine de l'affectation du NATINS, d'autant plus que Cassiopée est placé sous le contrôle du juge[2041].

1177. L'obstacle de situations transitoires à l'affectation initiale du NATINS par Cassiopée. – Néanmoins, il existe certaines situations, en nombre important, où un individu fait l'objet d'une saisie d'informations nominatives dans des traitements, avant Cassiopée. Par voie de conséquence, le code NATINS ne pourrait pas découler de Cassiopée dans ces cas-là. Tout d'abord, le cas le plus fréquent concernerait le TAJ dans lequel les officiers de police judiciaire créent une fiche pour toutes les personnes qu'ils entendent ou soupçonnent. Cette personne n'est pas encore connue dans Cassiopée à ce stade-là de l'enquête, puisque l'alimentation de Cassiopée suppose qu'une procédure judiciaire devant une juridiction pénale soit introduite[2042]. Ensuite, cela peut être le cas avec le fichier des personnes recherchées qui prévoit l'inscription en cas d'interdiction de sortie du territoire[2043]. Dans ce cas, l'inscription peut être ordonnée alors qu'il n'y pas encore eu de procédure ouverte dans Cassiopée. Enfin, cette situation peut se présenter

[2037] Annexe 4, projet de décret pris en application des dispositions relatives à la base nationale des données judiciaires, articles 11 à 17.
[2038] V. p.35
[2039] A savoir, les personnes mises en cause, condamnées ou recherchées, les témoins et les victimes, puisque le quatrième code correspond aux données de traçabilité. Ce dernier est affecté indépendamment car il concerne les utilisateurs de la BNDJ, ainsi que les avocats en tant qu'intervenants dans la procédure : v. *supra* n°1160.
[2040] V. annexe 5, cartographie actuelle, catégorie de données IV-A.
[2041] V. *supra* n°1172. *Op. cit.* p.35 BEGRANGER Gérald, *Le contrôle des fichiers de police par les juges*, Dalloz, AJ pénal 2014. p.176.
[2042] Sur le rôle de Cassiopée au sein des juridictions, v. LAVRIC Sabrina, *Parution du décret autorisant « Cassiopée »*, Recueil Dalloz 2009 p.1343.
[2043] C. pr. pén. art. 230-19 : « 14° L'interdiction de sortie du territoire prévue aux articles 373-2-6, 375-5, 375-7 et 515-13 du code civil ; »

avec le fichier automatisé des empreintes digitales ou le fichier national automatisé des empreintes génétiques, puisque le décret relatif à l'identification des personnes décédées[2044] prévoit une telle inscription sans qu'aucune procédure pénale n'ait été ouverte.

1178. La nécessité de prendre en compte ces situations transitoires. – Dans les trois situations qui viennent d'être évoquées, deux cas sont à distinguer. En premier lieu, lorsque l'inscription dans l'un des traitements judiciaires appelés à être hébergés dans la BNDJ se fait en dehors d'une procédure pénale, mais faisant suite à la décision d'une juridiction civile, les conditions de gestion du NATINS par l'autorité judiciaire seraient respectées. En effet, il suffirait d'apporter une modification mineure à Cassiopée pour que le juge civil puisse demander que les personnes inscrites dans ce cadre se voient affectées le code des personnes recherchées[2045]. Cette modification est prévue dans le projet de décret[2046].

1179. En second lieu, dans le cas du TAJ, la solution passerait par les paramètres techniques de la BNDJ. Il suffirait, lors de la définition des droits au sens informatique du terme, que les enquêteurs ne puissent créer de nouvelle fiche nominative qu'en attribuant le code NATINS de « témoin » ou de « victime ». En fonction de l'évolution du dossier, si une procédure est effectivement ouverte *a posteriori*, l'autorité judiciaire pourrait alors attribuer le NATINS de la catégorie des personnes mises en cause ou recherchées. Néanmoins, en cas d'urgence, lors de la communication qui existe entre les enquêteurs et les magistrats du Parquet[2047], les officiers de police judiciaires pourraient explicitement demander que le NATINS « personne mise en cause » soit affecté à tel ou tel individu pour lequel ils ont déjà créé une fiche.

1180. Conclusion du sous-paragraphe a : l'amélioration par l'introduction de codes transversaux. – Les sept traitements judiciaires dont l'hébergement dans la BNDJ est

[2044] Décret n°2012-125 du 30 janvier 2012 relatif à la procédure extrajudiciaire d'identification des personnes décédées.
[2045] Sur le descriptif des codes NATINS, v. *supra* n°1174.
[2046] V. annexe 4, projet de décret pris en application des dispositions relatives à la base nationale des données judiciaires, article 1 : « Dans l'énumération du 1° c) de l'article R15-33-66-6, après « dossier ; » est inséré : « , code de nature de l'inscription NATINS » qui vient modifier les dispositions relatives aux procédures civiles enregistrées par les parquets. » »
[2047] L'art. 54 du C. de pr. pén. pose comme un principe, en enquête de flagrance, l'échange entre l'officier de police judiciaire qui est informé d'un crime flagrant et le procureur de la République. Par suite, les articles 56 à 74-2 prévoient des échanges, notamment lorsque l'autorisation du procureur est nécessaire (v. par ex. C. pr. pén. art. 56).

proposé pourraient être améliorés en homogénéisant la donnée identifiant de manière unique une procédure et en affectant un même code aux personnes fichées déterminant à quel titre elles le sont.

1181. Plusieurs autres adaptations pourraient également contribuer à homogénéiser et améliorer la cohérence des données enregistrées dans ces fichiers.

b. Les adaptations pour améliorer la cohérence des données

1182. Des propositions d'homogénéisations. – L'analyse de la cartographie actuelle des informations contenues dans les traitements appelés à être hébergés au sein de la BNDJ[2048], met en évidence que des propositions de modifications seraient nécessaires pour rectifier le manque flagrant d'homogénéité des informations dans les différents fichiers[2049]. De telles modifications seraient une source de clarté et de lisibilité qui amélioreraient à la fois la transparence des traitements judiciaires, ainsi que leur efficacité en assurant la cohérence des données mises à la disposition des utilisateurs de ces fichiers. Ainsi, des améliorations sont proposées dans la suite des présentes, en suivant l'ordre des catégories classant les différentes informations contenues[2050].

1183. Le projet de cartographie améliorée[2051] regroupe l'ensemble des rectifications ainsi proposées, et permet donc de visualiser la cartographie des sept traitements judiciaires appelés à être hébergés par la BNDJ, matérialisant une cohérence améliorée et homogénéisée des données enregistrées.

1184. L'homogénéisation des données d'identification[2052]. – La cartographie actuelle met en évidence de nombreuses incohérences : des informations presque identiques, mais dénommées différemment d'un traitement à un autre[2053] ou encore une donnée qui est non explicitée dans un traitement alors qu'elle est tacitement utilisée[2054]. Les incohérences

[2048] V. supra n°1047. V. annexe 5, Cartographie issue des dispositions actuelles des traitements appelés à être hébergés par la BNDJ.
[2049] V. *supra* n°1169.
[2050] Sur les catégories choisies au sein de la cartographie, v. *supra* n°1153.
[2051] Annexe 6, projet d'amélioration de la cartographie des traitements appelés à être hébergés par la BNDJ.
[2052] Catégorie « I » : v. illustration n°7, p.35
[2053] V. par ex. le traitement d'antécédents judiciaires qui explicite « le surnom ou alias » (C. pr. pén. art. R40-26) et le fichier judicaire national automatisé des auteurs d'infractions terroristes qui parle de « changement de nom et nom d'usage » (C. pr. pén. art. R50-36).
[2054] Par ex. l'adresse dans le fichier des personnes recherchées (Décret n°2010-569 du 28 mai 2010 relatif au fichier des personnes recherchées, art. 3).

relatives aux données d'identification décrites ci-après devraient donc être rectifiées à l'occasion de la création de la BNDJ[2055].

1185. Seul le fichier national automatisé des empreintes génétiques ne comporte pas la donnée « sexe[2056] ». Il semble évident que toute analyse génétique donne cette information. Dans un souci de lisibilité et de cohérence, il serait opportun d'ajouter cette donnée.

1186. De même, le « surnom » et la « nationalité » ne sont pas présents dans les deux fichiers des empreintes[2057] ce qui constitue une incohérence qui mériterait d'être rectifiée.

1187. Etrangement, seul Cassiopée comporte la date de décès[2058]. Or, dans le cas où une personne fichée décède postérieurement à la procédure ayant conduit à son inscription dans l'un des traitements, il serait important que cette information soit clairement introduite. En effet, les traitements prévoient l'effacement des données lorsque le décès est connu[2059], ce qui semble contraire à l'efficacité de l'enquête. On voit désormais régulièrement des traces biologiques retrouvées bien des années après que des faits criminels ou délictueux se soient produits et, même si l'individu concerné est décédé entre temps, son identification peut faire avancer une enquête sur des personnes de son entourage, notamment en matière de criminalité organisée. En conséquence, il est proposé d'introduire la date de décès dans les sept traitements dont l'hébergement dans la BNDJ est proposé, et l'effacement systématique lors du décès d'un individu est supprimé[2060], à l'exception du fichier des personnes recherchées qui ne présente pas d'intérêt au-delà de la mort d'un individu.

1188. Il en est de même avec la langue parlée qui paraît absolument nécessaire pour l'ensemble des traitements[2061].

[2055] V. *infra* n°1192.

[2056] C. pr. pén. art. R53-11.

[2057] Le fichier automatisé des empreintes digitales (Décret n°87-249 du 8 avril 1987 relatif au fichier automatisé des empreintes digitales géré par le ministère de l'intérieur, art. 4) et le fichier national automatisé des empreintes génétiques (C. pr. pén. art. R53-11).

[2058] C. pr. pén. art. R15-33-66-6 : « […] dates de naissance et de décès […] ».

[2059] V. par ex. le fichier judiciaire national automatisé des auteurs d'infractions sexuelles ou violentes, C. pr. pén. art. R53-8-35 : « Le service gestionnaire du fichier procède à l'effacement des données qui y sont inscrites : […] Lorsqu'il est informé du décès de la personne ; […]. »

[2060] Annexe 4, projet de décret pris en application des dispositions relatives à la base nationale des données judiciaires, articles 14, 16 et 17 pour, respectivement, le fichier automatisé des empreintes digitales, le fichier judiciaire nationale automatisé des auteurs d'infractions sexuelles ou violentes et le fichier judiciaire national automatisé des auteurs d'infractions terroristes.

[2061] Cette donnée n'est actuellement prévue que dans Cassiopée (C. pr. pén. art. R15-33-66-6 : « […] langue, dialecte parlé ; […]. »

1189. Le champ « adresse » devrait être homogénéisé au sein des différents traitements. Tout d'abord, il est surprenant que tous les traitements ne comportent pas cette donnée pourtant essentielle[2062]. Ensuite, il existe des différences de formulation entre Cassiopée et le TAJ qui parlent « d'adresses » (au pluriel) ce qui sous-entend clairement « toutes les adresses connues », avec les deux traitements relatifs à des personnes dangereuses[2063] qui énoncent l'historique des adresses. Il est proposé d'homogénéiser les deux, sous la forme d'une information dénommée « Adresses » qui comporterait toutes les adresses connues, présentes et passées.

1190. Toujours au niveau des coordonnées, il semble essentiel de généraliser à tous les traitements l'adresse électronique ainsi que les numéros de téléphone[2064].

1191. Concrétisation des propositions des propositions de rectification. – Outre la rectification de la neutralisation par le décès d'une personne de la consultation de ses données contenues dans certains traitements[2065], le projet de décret pris pour l'application de la BNDJ concrétise l'ensemble de ces adaptations[2066].

1192. L'homogénéisation des éléments judiciaires pour les antécédents[2067]. – Dans la catégorie II, il est également proposé de rectifier plusieurs anomalies. Les adaptations des dispositions actuelles sont proposées dans le projet de décret de l'annexe 4[2068].

1193. Le signalement devrait être présent dans tous les traitements judiciaires[2069] appelés à être hébergés dans la BNDJ, à l'exception de Cassiopée en raison de la finalité administrative de suivi des procédures de celui-ci et non d'enquête[2070].

[2062] V. *supra* n°1184.
[2063] FIJAIS et FIJAIT.
[2064] Actuellement, seul Cassiopée et ponctuellement le TAJ contiennent ces informations.
[2065] V. *supra* n°1187. Les adaptations correspondantes sont traitées au sein des articles 14, 16 et 17 du projet de décret l'annexe 4.
[2066] Annexe 4, projet de décret pris en application des dispositions relatives à la base nationale des données judiciaires, articles 11 à 17.
[2067] Catégorie « II » : v illustration n°7, p.35
[2068] Les modifications sont retranscrites dans les articles 11 à 17 de l'annexe 4 (projet de décret pris en application des dispositions relatives à la base nationale des données judiciaires).
La proposition d'une cartographie améliorée de l'annexe 6 permet de visualiser l'amélioration qui en découle pour les données enregistrées sans les sept traitements.
[2069] Actuellement, seuls le traitement d'antécédents judiciaires (C. pr. pén. art. R40-26) et le fichier des personnes recherchées (Décret n°2010-569 du 28 mai 2010 relatif au fichier des personnes recherchées, art. 3) contiennent cette donnée.
[2070] La consultation de Cassiopée ne constitue pas une investigation numérique : v. *supra* n°625.

1194. Les photos anthropométriques[2071] et les photos permettant la reconnaissance faciale[2072] devraient être regroupées en une seule donnée, car ces dernières constituent une évolution technologique des premières. Par ailleurs, ce type de photo devrait être présente dans le fichier des personnes recherchées, celui des empreintes génétiques ainsi que dans les deux traitements s'intéressant à des auteurs d'infractions présentant potentiellement un haut degré de dangerosité[2073].

1195. L'homogénéisation des éléments factuels de la procédure en cours[2074]. – Des données identiques sont enregistrées sous des noms différents dans les traitements appelés à être hébergés au sein de la BNDJ : « faits-description » pour Cassiopée, le TAJ (au sein duquel vient s'ajouter le champ « objets de l'enquête ») et le fichier automatisé des empreintes digitales, « nature de l'affaire » pour celui des empreintes digitales, « motifs de la recherche » pour le fichier des personnes recherchées, et « nature de l'infraction » au sein des FIJAIS et FIJAIT[2075].

1196. Pour ces deux derniers traitements, l'inscription au fichier peut être réalisée bien avant qu'une condamnation définitive n'ait été prononcée[2076], ce qui confirme qu'il s'agit plus de la nature des faits qui aboutit à l'inscription qu'une condamnation. Celle-ci est, par ailleurs, présente dans des champs du suivi judiciaire de la procédure en cours. Il serait possible d'homogénéiser toutes ces informations en les regroupant sous une même dénomination : « Faits – Description infraction[2077] ».

1197. L'homogénéisation des données relatives au suivi judiciaire d'une procédure[2078]. – Outre l'officialisation du numéro de procédure issu de Cassiopée au sein des sept traitements judiciaires dont l'hébergement est proposé dans la BNDJ[2079] et

---

[2071] V. par ex. le fichier automatisé des empreintes digitales (Décret n°87-249 du 8 avril 1987 relatif au fichier automatisé des empreintes digitales géré par le ministère de l'intérieur, art. 4).
[2072] V. par ex. le traitement d'antécédents judiciaires (C. pr. pén. art. R40-26).
[2073] FIJAIS et FIJAIT.
[2074] Catégorie « III » : v. illustration n°7, p.35
[2075] C. pr. pén. art. R53-8-7 et R50-36 : « Nature de l'infraction ou des infractions pour lesquelles la personne est poursuivie ou condamnée. »
[2076] V. resp. C. pr. pén. art. 706-53-2 : « […] sont enregistrées dans le fichier les informations relatives à […] des personnes ayant fait l'objet : […] 1° D'une condamnation, même non encore définitive […] 5° D'une mise en examen […]. »
C. pr. pén. art. 706-25-4 : *idem.*
[2077] Annexe 4, projet de décret pris en application des dispositions relatives à la base nationale des données judiciaires, articles 13 et 15 et annexe 6 pour le projet de cartographie améliorée.
[2078] Catégorie « IV » : v. illustration n°7, p.35
[2079] V. *supra* n°1172.

l'intégration du code NATINS[2080], l'analyse de la cartographie révèle que des informations identiques sont présentes sous des noms différents ou bien se recoupent au sein des différents fichiers. Plusieurs homogénéisations pour cette catégorie de données sont donc nécessaires. Elles sont décrites ci-après et les adaptations correspondantes des dispositions actuelles sont proposées dans le projet de décret de l'annexe 4[2081].

1198. La donnée « date et historique des condamnations » devrait remplacer « date de condamnation définitive[2082] », « date condamnation[2083] », « nature du jugement[2084] », « date jugement[2085] » ainsi que « juridiction décision[2086] ».

1199. La donnée « fin peine/mesure/exécution » est une particularité du FIJAIS[2087]. Elle pourrait être supprimée car cette donnée devrait faire explicitement partie des informations relatives à la « peine prononcée ».

1200. L'homogénéisation des informations relatives aux intervenants dans la procédure[2088]. – L'analyse de la cartographie actuelle appelle une modification et une précision.

1201. En premier lieu, il est important de souligner que cette catégorie d'informations comporte les données relatives à la traçabilité. Le cadre général de création de la BNDJ[2089] propose la création de dispositions officialisant la collecte de données à caractère personnel des utilisateurs des traitements[2090]. Les dispositions des sept traitements appelés à être bébergés par la BNDJ devraient être adaptées afin d'établir une cohérence avec la BNDJ, puisque la gestion de la traçabilité des traitements hébergés serait désormais intégrée dans celle-ci. Le projet de décret intègre les adaptations

[2080] V. *supra* n°1174.
[2081] Annexe 4, projet de décret pris en application des dispositions relatives à la base nationale des données judiciaires, articles 11, 15, 16 et 17.
[2082] Fichier national automatisé des empreintes génétiques, C. pr. pén. art. R53-14.
[2083] *Ibid.*
[2084] V. par ex. Cassiopée (C. pr. pén. art. R15-33-66-6) ou le fichier judicaire national automatisé des auteurs d'infractions sexuelles ou violentes (C. pr. pén. art. R53-8-7).
[2085] Fichier judicaire national automatisé des auteurs d'infractions sexuelles ou violentes (C. pr. pén. art. R53-8-7).
[2086] *Ibid.*
[2087] Fichier judicaire national automatisé des auteurs d'infractions sexuelles ou violentes (C. pr. pén. art. R53-8-7 : « […] -date d'exécution ou de fin d'exécution de la peine ou de la mesure ; […]. »
[2088] Catégorie « VI » : v. illustration n°7, p.35
[2089] V. *supra* n°1126.
[2090] V. *supra* n°1134.

correspondantes[2091]. Par ailleurs, la cartographie actuelle des traitements judiciaires, objet de l'annexe 5, montre que seul Cassiopée explicite clairement que des données personnelles relatives à l'agent de la fonction publique d'état qui saisit les données d'une procédure, sont collectées[2092]. Les deux fichiers relatifs aux empreintes s'intéressent au service ayant procédé au signalement[2093], sans préciser que les personnes intervenant sur les données font l'objet d'une traçabilité nominative, ce qui est nécessairement le cas. D'autres traitements comportent évidemment ces informations, sans qu'elles soient listées dans les données enregistrées[2094]. En conséquence, il est proposé d'homogénéiser l'ensemble de ces informations sur la base de ce qu'énonce Cassiopée, en employant le terme générique « d'opérateur » pour couvrir, à la fois, les agents et les militaires. Cette proposition de modification de la cartographie[2095] est concrétisée au travers du projet de décret de l'annexe 4 pour l'adaptation des deux traitements des empreintes[2096]. Les autres fichiers seraient visés par le nouvel article R40-59 qui liste les données enregistrées au titre de la traçabilité pour l'ensemble des traitements hébergés par la BNDJ[2097].

1202. En second lieu, une précision doit être apportée au sein de cette catégorie de données relatives aux intervenants dans une procédure. Cassiopée possède une spécificité en adéquation avec sa finalité du suivi du déroulé des procédures : toutes les informations nominatives relatives aux avocats assurant la défense des différentes parties prenantes y sont présentes[2098]. La présente étude propose que le régime de ces données soit assimilé,

---

[2091] Annexe 4, projet de décret pris en application des dispositions relatives à la base nationale des données judiciaires, article 2 venant modifier l'art. R40-30 du C. pr. pén. relatif au traitement d'antécédents judiciaires.
Article 3 venant modifier l'art. R15-33-66-13 du C. pr. pén. relatif à Cassiopée.
Article 4 venant modifier le décret n°2010-569 du 28 mai 2010 relatif au fichier des personnes recherchées.
Article 7 venant modifier l'art. R53-8-34 du C. pr. pén. relatif au fichier judiciaire national automatisé des auteurs d'infractions sexuelles ou violentes.
Article 8 venant modifier l'art. R50-63 du C. pr. pén. relatif au fichier judiciaire national automatisé des auteurs d'infractions terroristes.

[2092] C. pr. pén. art. R15-33-66-6 : « […] Concernant le personnel du ministère de la justice :
-nom de naissance ou d'usage et prénom ;
-corps et/ou grade, fonction ;
-code position administrative de l'agent, mnémonique du service de l'agent, libellé du service. »

[2093] V. par ex. le fichier national automatisé des empreintes génétiques, C. pr. pén. art. R53-11 : « […] 2° L'autorité judiciaire ou l'officier de police judiciaire ayant demandé l'enregistrement au fichier […]. »

[2094] Par ex. le fichier des personnes recherchées. Le rapport Batho/Benisti (*op. cit.* p. 35) précise à son sujet que « il apparaît que ces conduites à tenir manquent souvent de précision et de clarté, ce qui oblige le service inscripteur à entrer en contact avec les services demandeurs. » (p. 95 du rapport). On en déduit que les agents et militaires qui utilisent le fichier ont connaissance du service inscripteur.

[2095] V. annexe 6 projet de cartographie améliorée.

[2096] Annexe 4, projet de décret pris en application des dispositions relatives à la base nationale des données judiciaires, articles 14 et 15.

[2097] V. *supra* n°1136.

[2098] V. *supra* n°1160.

dans ses effets, aux informations de traçabilité. Cela assurerait ainsi aux avocats que leurs données personnelles soient protégées lors des recherches au sein des fichiers hébergés par la BNDJ, au même titre que celles des opérateurs qui interviennent sur les différents traitements.

1203. Conclusion du sous-paragraphe I : le régime des traitements hébergés au sein de la BNDJ. – Parmi l'ensemble des traitements judiciaires actuels, la présente étude propose que sept traitements soient hébergés au sein de la Base Nationale de Données Judiciaires[2099]. L'analyse exhaustive de la cartographie des données contenues dans ces traitements a deux intérêts. En premier lieu, elle permet d'identifier avec précision quelles données pourraient être mises en commun pour ces sept traitements et qu'elles sont celles qui devraient rester totalement étanches. En second lieu, la cartographie révèle de multiples incohérences et des lacunes. Ainsi, une cartographie améliorée est proposée afin d'homogénéiser et de rationaliser les données contenues dans les différents traitements hébergés. Le projet de décret objet de l'annexe 4 contient les modifications des dispositions actuelles correspondantes.

1204. La BNDJ est un outil technique qui a vocation à dépasser les seuls traitements qu'elle pourrait héberger. En effet, certains fichiers, qui ne peuvent pas être hébergés par celle-ci, notamment en raison de leur finalité, pourraient être liés à la BNDJ afin de poursuivre l'amélioration et la rationalisation des données contenues dans ces traitements malgré le fait qu'ils demeurent physiquement séparés.

II – <u>Le régime des traitements liés à la BNDJ</u>

1205. La création d'un lien informatique avec les traitements autonomes. – La proposition de créer une Base Nationale de Données Judiciaires dépasse la seule fonction d'héberger des traitements judiciaires[2100]. Une seconde fonction pourrait prolonger l'objectif de celle-ci d'améliorer la qualité des informations dans le plus grand nombre possible de traitements mis en œuvre par l'état. Pour cela, il est proposé d'établir un lien informatique entre les données de la BNDJ et celles de traitements restant physiquement séparés[2101], lorsqu'il existe une pertinence à procéder à des mises à jour avec les

[2099] V. *supra* n°1149.
[2100] *Ibid.*
[2101] V. l'ensemble des traitements administratifs (v. *supra* n°697.) ou des fichiers dédiés au renseignement (v. *supra* n°709.) pour lesquels un accès direct est prévu pour les autorités judiciaires au stade de l'enquête pénale (v. *supra* n°612.).

informations de la BNDJ. Bien évidemment, en aucun cas, les données de la catégorie « V »[2102], constituant le cœur des traitements judiciaires, ne doivent être concernées par de telles mises à jour.

Il est nécessaire d'étudier la faisabilité d'un tel lien dans le respect du cadre légal général énoncé pour la BNDJ *(A)*, avant de pouvoir déterminer, parmi les traitements judiciaires non intégrés à la BNDJ, quels sont ceux qui pourraient être liés avec celle-ci *(B)*.

A. La possibilité d'un lien informatique entre la BNDJ et des traitements séparés

1206. La convergence entre la notion juridique d'interconnexion et la notion informatique d'interopérabilité. – La situation de logiciels différents, qui cohabitent au sein d'un même système d'information et qui s'échangent des informations est fréquente en informatique[2103], afin d'éviter les re-saisies de données identiques, sources d'erreurs importantes[2104], et d'assurer le maximum de cohérence entre les informations enregistrées dans l'ensemble des traitements[2105]. La mise en relation de deux bases de données, leur permettant de s'échanger des informations, est qualifiée d'interopérabilité en informatique. Outre la définition scientifique de l'interopérabilité[2106], celle-ci permettrait à un traitement judiciaire restant physiquement séparé de la BNDJ, de pouvoir échanger avec cette dernière, au travers d'une interface commune, des informations définies. Techniquement, cette interopérabilité est synonyme de synchronisation de données préalablement listées. Juridiquement, l'interopérabilité est intégrée dans la notion d'interconnexion qui est issue du droit de la protection des données personnelles[2107].

[2102] V. *supra* n°1159.

[2103] Sur les raisons de la présence de plusieurs bases de données au sein d'un même système d'information, v. *supra* n°1055.

[2104] V. *supra* n°1048. *Op. cit.* Ministère de la justice du Quebec, bureau de la sous-ministre et sous-procureure générale, *Plan directeur en ressources informationnelles du ministère*, 17 décembre 2019 : « Intégration inadéquate de l'information de justice : La désuétude des systèmes informatiques conduit à une difficile intégration de l'information entre les entités et les systèmes, ce qui oblige trop souvent la saisie multiple d'une même information. »

[2105] Sur la nécessité d'une gestion des données centralisée aux fins d'en assurer la cohérence et la fiabilité, v. DUTHEIL Christophe, *L'usine du futur s'édifie brique par brique,* ElectroniqueS n°64, 1er octobre 2015.

[2106] INTEROP-Vlab, *Secured exchanges of data along the logistic chains,* 7 octobre 2015 : Interoperability is the ability of […] a system or […] software (ERP…) to interact with others at a low cost in a flexible approach.

[2107] V. *supra* n°1093.

1207. Les différents degrés de l'interopérabilité[2108]. – Il existe deux degrés à la synchronisation des informations entre des bases de données différentes : l'interopérabilité semi-automatique et automatique. L'interopérabilité automatique suppose, pour la liste des données définies, que la création ou la modification d'une information dans une base de données est systématiquement répercutée dans l'autre base, sans aucune intervention humaine. Dans l'exemple du système d'information de santé[2109] précédemment développé[2110], l'interopérabilité entre le logiciel qui gère les admissions d'un établissement hospitalier et le dossier patient informatisé est automatique. Ce dernier est asservi au logiciel administratif. Avec l'interopérabilité semi-automatique, lorsqu'une information est créée ou mise à jour dans une base de données, un message[2111] est envoyé à un modérateur qui peut-être un opérateur ou un administrateur, et qui peut décider, au travers d'une validation, d'accepter que cette création ou mise à jour soit répercutée dans l'autre base ou pas. L'utilisation de ces deux degrés d'interopérabilité est utile pour proposer d'établir un lien entre la BNDJ et certains traitements de données.

1208. La légalisation d'une interconnexion automatique pour tous les traitements hébergés au sein de la BNDJ fait l'objet d'une disposition prévue par le chapitre deux, de la proposition de loi visant à améliorer l'efficacité et à renforcer les garanties des traitements de données en procédure pénale, dédié à la BNDJ[2112]. L'interconnexion de cette dernière avec des fichiers physiquement séparés au travers en utilisant une interopérabilité informatique doit également être légalisée[2113].

B. La création d'un lien informatique entre la BNDJ et des traitements séparés

1209. La détermination des traitements séparés et liés à la BNDJ. – L'informatique offre des moyens techniques permettant de mettre en œuvre une interopérabilité maîtrisée

[2108] REZAEI Reza, CHIEW Thiam-kian, LEE Sai-peck, *A review of interoperability assessment models,* Journal of Zhejiang University-SCIENCE C, www.springerlink.com, 2013 : « […] interoperability is normally related to the definition of content, and deals with the human, rather than machine, interpretation of this content. »

[2109] Sur la nécessité d'interopérabilité dans les systèmes d'information de santé, v. Le Quotidien du Médecin, *Politique de santé - Gouvernance renforcée, déploiement de services digitaux - Le gouvernement veut accélérer sur le numérique en santé*, Le Quotidien du médecin, 20 janvier 2020.

[2110] V. *supra* n°1056.

[2111] Les informaticiens parlent de « notification ».

[2112] V. *supra* n°1096.

[2113] Annexe 2, proposition de loi, article 10, nouvel art. 230-49, second alinéa : « La même interconnexion technique peut être mise en œuvre avec un autre traitement de données, afin de permettre l'identité des informations présentes dans la base nationale de données judiciaires avec celles de ce traitement. »

entre des bases de données séparées. Le cadre légal permettant de créer celle-ci repose sur la notion d'interconnexion.

1210. Pour autant, parmi l'ensemble des traitements de données accessibles en enquêtes, beaucoup doivent rester totalement autonomes *(1)*. Lorsque l'interconnexion pour certains fichiers s'avèrerait pertinente *(2)*, les critères et le degré d'interopérabilité doivent être précisément définis.

1. Des critères pour lier certains traitements judiciaires

1211. La continuité de la règle d'un rapprochement mesuré. – Comme précédemment expliqué, il ne serait pas réaliste de proposer une mise en commun des données de l'ensemble des traitements directement accessibles au stade de l'enquête[2114]. Même dans le cas d'une interopérabilité où un fichier resterait physiquement séparé de la BNDJ, la règle d'une séparation totale pour certains traitements se prolongerait, car plusieurs critères imposent qu'une totale autonomie soit maintenue pour de nombreux fichiers.

1212. Le critère d'une base faisant foi. – Certes, il est proposé que le service du Casier judiciaire assure la mise en œuvre opérationnelle et la supervision de la BNDJ[2115]. Cependant, le Casier judiciaire en tant que traitement de données doit rester une base entièrement autonome car il est important de préserver l'aspect « figé » qui est le sien et qui fait foi en matière de condamnations[2116]. Il doit être déconnecté de toutes les procédures en cours, et se limiter à contenir les informations relatives aux décisions effectivement prononcées par des juridictions pénales. Concrètement, l'interrogation du Casier judiciaire n'est pas une investigation numérique[2117].

1213. Le critère de personnes éloignées de la délinquance ou de la criminalité. - Tous les traitements en rapport avec les véhicules, les objets volés ou relatifs aux infractions au Code de la route[2118] doivent également rester totalement autonomes. Les

[2114] V. *supra* n°965.
[2115] V. *supra* n°1112.
[2116] GRUNVALD Sylvie, *Casier judiciaire et effacement des sanctions : quelle mémoire pour la justice pénale ?* Dalloz AJ pénal 2007 p.416 : « Le casier judiciaire est communément présenté comme la mémoire de la justice pénale, […]. »
BADINTER Robert, *Discours d'inauguration du Casier judiciaire*, 8 juin 1982 : « Le casier judiciaire, c'est mémoire douloureuse de la justice. »
[2117] V. *supra* n°642.
[2118] V. supra n°678.

données personnelles enregistrées dans ces fichiers ne concernent pas des actes délictuels ou criminels. Ainsi, il serait difficilement justifiable qu'une personne se retrouve fichée dans la BNDJ (tout particulièrement en qualité de personne condamnée) pour, par exemple, une infraction au Code de la route[2119]. Aucune interopérabilité entre ces fichiers et la BNDJ se serait souhaitable car ces traitements contiennent des informations qui ne sont utiles à une enquête que de manière très ponctuelle et dans des cas particuliers[2120].

1214. Le critère de traitements propres à des investigations numériques autonomes. – Il existe au sein de la procédure pénale une confusion entre les analyses de données recueillies au cours de l'enquête et les traitements de données à caractère personnel mis en œuvre dans le cadre d'une investigation numérique[2121]. En effet, certains actes, comme les analyses de disques durs ne sont pas considérés, par la procédure, comme générant un traitement de données tandis que les investigations numériques créées plus récemment sont associées à un traitement dument déclaré. Pour toutes ces investigations numériques, pour lesquelles le traitement est inextricablement associé à l'exploitation des données collectées, la liaison avec la BNDJ ne se conçoit pas. Il s'agit des écoutes téléphoniques[2122], des données captées[2123] ainsi que des logiciels d'analyse sérielle et de rapprochement judiciaire[2124].

1215. Le même critère impose qu'aucune mise à jour ne soit envisagée avec les traitements de données correspondant au PSE, au PSEM[2125] ainsi qu'au REDEX[2126]. En effet, ces fichiers sont principalement dédiés à l'exécution et au suivi de condamnations ou de mesures ordonnées par une autorité judiciaire. En ce sens, leur spécialisation produit les mêmes effets que les traitements déclarés pour des investigations numériques spécifiques : leurs données doivent rester propres au périmètre qui leur est défini. Par ailleurs, dans le cas particulier du REDEX, qui concerne le suivi de la dangerosité de

[2119] Pour les traitements de données mis en œuvre pour les infractions au Code de la route, v. *supra* n°679.
Arrêté du 13 octobre 2004 portant création du système de contrôle automatisé.
Arrêté du 2 décembre 2010 autorisant la mise en œuvre d'un traitement automatisé d'information à caractère personnel pour la gestion des amendes forfaitaires et des consignations dénommé « Gestion des amendes forfaitaires des unités élémentaires de la gendarmerie départementale et des gendarmeries spécialisés ».
[2120] *Ibid.*
[2121] V. *supra* n°805.
[2122] V. *supra* n°687.
[2123] V. *supra* n°692.
[2124] V. *supra* n°720.
[2125] V. *supra* n°658.
[2126] V. *supra* n°672.

personnes déjà condamnés pour des faits graves[2127], les informations rappelant les antécédents sont nécessairement présentes dans d'autres traitements tels qu'*a minima*, le TAJ et Cassiopée[2128]. Par voie de conséquence elles sont accessibles, pour les autorités judiciaires, grâce à d'autres fichiers appelés à être hébergés par la BNDJ.

2. Le périmètre pour définir les traitements liés

1216. Une interconnexion parfaitement maîtrisée. – La création d'une interopérabilité entre certains fichiers qui doivent rester physiquement séparés et la BNDJ ne pourrait se faire que dans le respect d'un périmètre encadré[2129]. Le degré d'interopérabilité et, surtout, le sens de la communication doivent être parfaitement définis. Le sens de la communication détermine que seules les mises à jour ou les créations d'une base peuvent être répercutées dans l'autre. Les modifications de cette dernière peuvent être sans effet sur l'autre base de données. Cette façon de fonctionner est utile avec des traitements de police administrative qui n'ont pas vocation à modifier les informations de fichiers judiciaires, mais pour lesquels une interopérabilité serait nécessaire tant les traitements administratifs jouent désormais un rôle essentiel *(b)*.
Auparavant, une première interconnexion devrait être envisagée avec les logiciels servant de support à la rédaction des procès-verbaux pour les officiers de police judiciaire *(a)*.

a. Les logiciels pour la rédaction des procès-verbaux

1217. Un outil de travail intégré dans le quotidien des enquêteurs. – Les LRPPN et LRPGN sont les logiciels de rédaction des procès-verbaux pour la Police et la Gendarmerie[2130]. A ce titre, ils ne pourraient pas être hébergés par la BNDJ car ils sont en quelque sorte le logiciel bureautique des OPJ et ils doivent donc rester sous le contrôle

[2127] Auxquelles il faut ajouter les personnes ayant bénéficié d'un acquittement ou d'une relaxe pour cause d'irresponsabilité pénale, C. pr. pén. art. 706-56-2 : « […] Durant le déroulement d'une mesure de soins psychiatriques ordonnée en application de l'article 706-135 du présent code ou de l'article L. 3213-7 du code de la santé publique.
En cas de décision de classement sans suite, hormis les cas où cette décision est fondée sur le premier alinéa de l'article 122-1 du code pénal, ou de décision définitive de non-lieu, de relaxe ou d'acquittement, les données concernant la personne poursuivie sont immédiatement effacées. […]. »
[2128] V. annexe 5, cartographie issue des dispositions actuelles des traitements appelés à être hébergés par la BNDJ.
[2129] Notamment dans le respect de la traçabilité des actions (v. *supra* n°1133.). Sur la nécessité et la faisabilité technique d'assurer la traçabilité dans un contexte d'interopérabilité : v. BREBION Patrick, *La traçabilité dans les filets de Findus*, It for Business, 1er janvier 2015 : « Pour orchestrer les briques d'un système d'information hétérogène et s'interfacer facilement avec ses partenaires, Findus a opté pour la mise en place d'un service d'intégration de tous ses flux de données, assurant une traçabilité sans faille. »
[2130] V. *supra* n°649.

total des enquêteurs. Pour autant, les autorités publiques ont pris conscience de l'importance des mises à jour des données entre ces deux applications et Cassiopée, puisque des interconnexions sont d'ores et déjà opérées[2131]. Avec le projet de création d'une entité regroupant certains traitements judiciaires, il est proposé d'aller plus loin en créant une interopérabilité forte entre ces deux logiciels et la BNDJ car, de nombreuses informations sont communes.

1218. La priorité laissée aux juges pour la BNDJ. – Grâce au projet de cartographie améliorée[2132] et à la liste des données déclarées pour le LRPPN[2133] et pour le LRPGN[2134], il est possible de proposer deux types d'interopérabilité.

En premier lieu, une interconnexion fonctionnant dans les deux sens de manière automatique, concernerait les données de la catégorie « I » de la BNDJ[2135] telles que, par exemple, l'adresse ou l'identification des personnes. Ces informations devraient absolument pouvoir bénéficier de toutes les possibilités d'actualisation. L'efficacité de l'enquête pénale ne pourrait qu'en être améliorée, d'autant plus que ces informations ne sont pas critiques pour les droits des personnes fichées.

En second lieu, une interopérabilité semi-automatique est proposée pour les catégories II, III, IV-A, ainsi que pour les informations de traçabilité VI-B[2136]. En effet, ces dernières ont une correspondance directe avec les données collectées par le LRPPN et le LRPGN[2137]. La remontée de ces informations de traçabilité vers la BNDJ pourrait s'avérer utile lorsqu'une mise à jour des données de celle-ci serait issue de l'un de ces deux logiciels car, *a posteriori*, cela pourrait renseigner un enquêteur sur les dernières actions connues d'un individu fiché. Pour toutes les autres informations de ce second groupe de données, la mise à jour pourrait être automatique dans le sens BNDJ vers LRPPN et LRPGN, mais ne devrait être que semi-automatique[2138] dans l'autre sens. En effet, il est essentiel que les informations présentes dans la BNDJ soient placées sous le

---

[2131] V. *supra* n°625.
[2132] V. annexe 6.
[2133] Annexe du 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).
[2134] Article 2 du décret n°2011-111 du 27 janvier 2011 autorisant la mise en œuvre par le ministère de d'intérieur (direction générale de la gendarmerie nationale) d'un traitement automatisé de données à caractère personnel d'aide à la rédaction des procédures (LRPGN).
[2135] V. *supra* n°1155.
[2136] *Ibid.*
[2137] V. art. 5 et art. 6 des décrets du 27 janvier 2011 *(Ibid.)* pour, resp. le LRPPN et le LRPGN.
[2138] Comme expliqué précédemment, au travers d'un message d'information qui est remonté au gestionnaire du traitement lui laissant la faculté d'accepter ou de refuser la mise à jour qui lui est signalée.

contrôle du pouvoir judiciaire et non des enquêteurs[2139], ce qui serait le cas si les LRPPN et LRPGN venaient automatiquement mettre à jour des données relatives aux faits de la procédure.

1219. La proposition de créer cette interopérabilité doit être prévue dans les textes encadrant ces deux logiciels. Or, étrangement, seul le décret du LRPGN s'intéresse à la notion d'interconnexion[2140], en faisant référence au JUDEX qui n'existe plus puisqu'il a été remplacé par le traitement d'antécédents judiciaires[2141]. Des modifications des deux décrets correspondants au LRPPN et le LRPGN pour légaliser la mise en relation des données sont proposées[2142].

b. Les fichiers de police administrative

1220. L'importance des fichiers administratifs dans la mise à jour des informations. – Tous les traitements administratifs à vocation de maintien de l'ordre et de sécurité publique[2143] ne devraient pas être hébergés par la BNDJ. Ils devraient rester indépendants en raison de leur finalité non judiciaire. En revanche, postérieurement à la vague d'attentats ayant frappé la France et les autres pays européens, le pouvoir administratif dans le maintien de l'ordre a considérablement été étendu. Ainsi, outre l'accès directement prévu pour les enquêteurs à ces traitements administratifs lors d'une enquête pénale, la probabilité pour que les informations contenues dans ces fichiers soient plus fréquemment mises à jour que dans les traitements judiciaires est importante.

1221. L'apport positif d'une interopérabilité mesurée et définie. – En conséquence, une interconnexion entre les fichiers administratifs et la BNDJ pourrait améliorer significativement la qualité des données de cette dernière. Avec les traitements administratifs, la mise à jour ne devrait pas être automatique car il serait choquant qu'un

---

[2139] V. *supra* n°1172.

[2140] *Ibid.* art. 4 : « L'application « LRPGN » peut être mise en relation avec le système judiciaire d'exploitation (JUDEX) autorisé par le décret du 20 novembre 2006 susvisé par la transmission, en vue de son alimentation, des données relatives aux procédures judiciaires. »

[2141] V. *supra* n°153.

[2142] Annexe 4, projet de décret pris en application des dispositions relatives à la base nationale des données judiciaires, article 9 venant modifier 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).
Article 10 venant modifier le décret n°2011-111 du 27 janvier 2011 autorisant la mise en œuvre par le ministère de l'intérieur (direction générale de la gendarmerie nationale) d'un traitement automatisé de données à caractère personnel d'aide à la rédaction des procédures (LRPGN).

[2143] V. *supra* n°706.

traitement administratif impose une modification dans une base de données judiciaire. En revanche, le mécanisme de l'interopérabilité semi-automatique[2144] serait parfaitement adapté puisque la mise à jour d'une information telle qu'un changement d'adresse dans l'un des fichiers administratifs, enverrait une alerte aux administrateurs de la BNDJ qui, au travers d'une action volontaire, valideraient ou refuseraient que la modification soit opérée dans les données des traitements judiciaires. Le projet de cartographie améliorée[2145] permet d'étudier, avec la liste des données indiquées dans le Code de la sécurité intérieure[2146] pour chaque traitement, les informations de la catégorie « I » de la BNDJ[2147] qui pourraient faire l'objet d'une interopérabilité.

1222. La définition précise des informations liées. – Parmi les fichiers administratifs dédiés à la sécurité publique et au maintien de l'ordre, quatre traitements présentent un intérêt majeur pour améliorer la qualité de l'actualisation des données de la BNDJ. La mise en place d'une interconnexion entre cette dernière et les quatre fichiers administratifs est matérialisée sur l'illustration n°8.

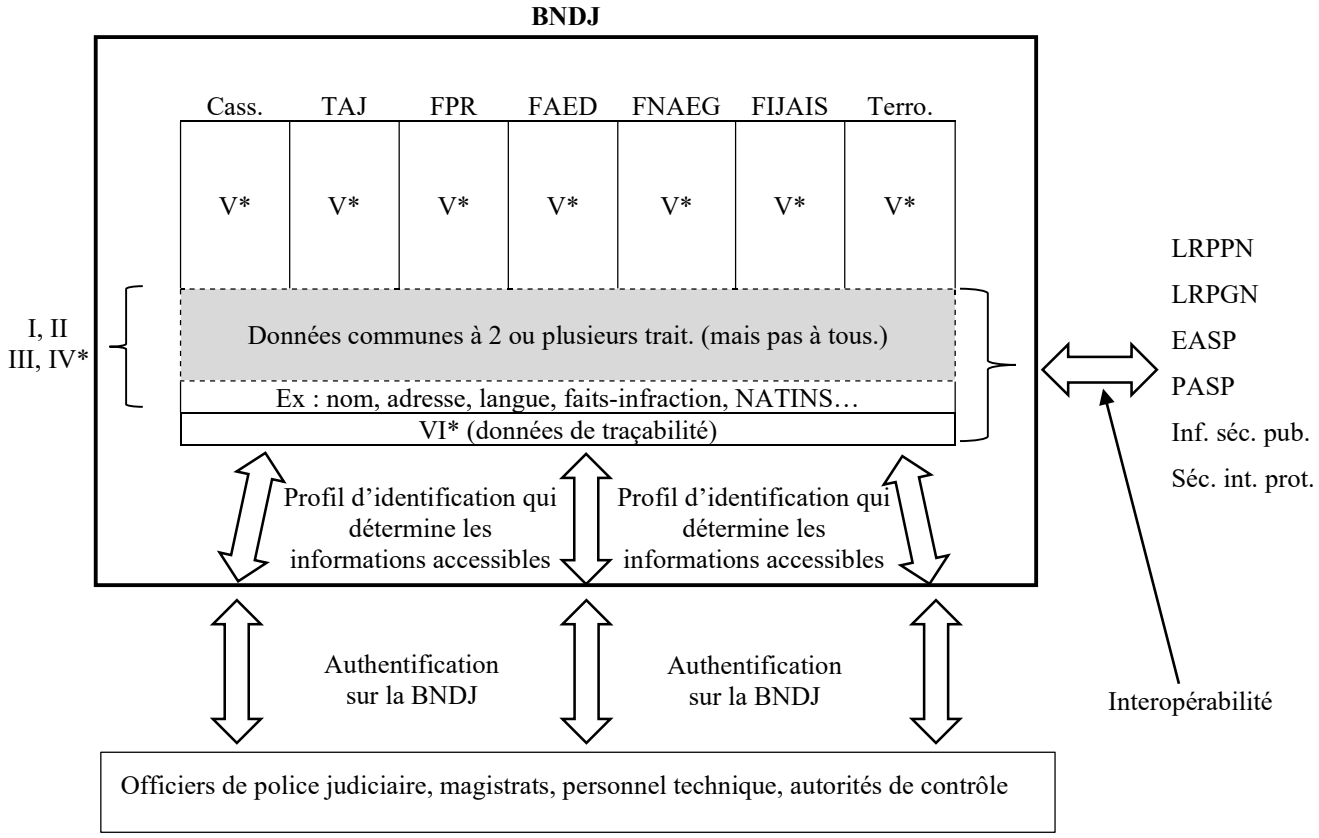
1223. En premier lieu, l'EASP[2148] répond à cet intérêt pour la BNDJ. En effet, à la lecture de l'article R236-2 du Code de la sécurité intérieure qui liste les données collectées, il est proposé une interopérabilité semi-automatique avec la BNDJ pour, d'une part, la profession, les adresses physiques, les numéros de téléphone et les adresses électroniques et, d'autre part, les photographies.

1224. En deuxième et troisième lieu, ce sont le PASP[2149] et le traitement « gestion de l'information et prévention des atteintes à la sécurité publique[2150] » qui sont pertinents. Les articles R236-12 et R236-22 du même Code montrent que les informations suivantes pourraient être soumises à une validation de synchronisation. Tout d'abord, la nationalité, la profession, les adresses physiques, les numéros de téléphone et adresses électroniques pourraient être synchronisées sous réserve de validation. Ensuite, il pourrait en être de même avec les signes physiques particuliers et objectifs[2151] et les photographies.

[2144] V. *supra* n°1207.
[2145] V. annexe 6.
[2146] Code la sécurité intérieure, Partie réglementaire, Livre II : Ordre et sécurité publics, Titre III : Traitements automatisés de données personnelles et enquêtes administratives, art. R231-1 et s.
[2147] Les données d'identification, v. *supra* n°1155.
[2148] Traitement automatisé de données à caractère personnel dénommé « Enquêtes administratives liées à la sécurité publique ». V. *supra* n°709.
[2149] Traitement de données à caractère personnel dénommé « Prévention des atteintes à la sécurité publique ». *Ibid.*
[2150] *Ibid.*
[2151] En correspondance avec la donnée « signalement » présente dans la BNDJ.

1225. En quatrième lieu, le fichier « sécurisation des interventions et demandes particulières de protection[2152] » est intéressant pour deux types de données qui ressortent de la lecture de l'article R236-39 du même Code, et qui pourraient être synchronisées selon le même principe. Tout d'abord, la nationalité, la profession et les photographies constitueraient un premier groupe. Ensuite, ce seraient les adresses physiques, les numéros de téléphone et les adresses électroniques qui sont relatives aux coordonnées.

1226. L'inutile proposition d'adaptation des dispositions existantes. – L'interconnexion envisagée avec ces quatre fichiers ne nécessiterait aucune intervention par voie règlementaire puisque les traitements concernés ne comportent pas de dispositions interdisant l'interconnexion.



(*)
I : Données identification
II : Eléments judiciaires pour les antécédents
III : Les éléments factuels de la procédure
IV : Le suivi judiciaire de la procédure
V : Données spécifiques aux traitements particuliers
VI : Informations relatives aux intervenants dans la procédure

Illustration n°8 : architecture de la BNDJ avec une interopérabilité vers des traitements externes

[2152] V. *supra* n°714.

1227. Conclusion du paragraphe §2 : l'évolution nécessaire du régime des traitements judiciaires avec la BNDJ. – L'illustration n°8 montre la structure complète proposée pour la BNDJ. Cette dernière permettrait de maintenir un cloisonnement étanche entre les données sensibles constituant le cœur des sept traitements judiciaires qui pourraient être hébergés en son sein, tout en permettant de regrouper les données communes à un ou plusieurs de ces traitements. De plus, une interface permettrait de prolonger la qualité des informations numériques enregistrées dans d'autres bases de données, notamment à vocation de police administrative, en créant une interconnexion avec la BNDJ. Cette interconnexion permettrait une mise à jour des données, soit automatiquement, soit de manière semi-automatique, c'est-à-dire moyennant la validation par un intervenant des autorités judiciaires. Le régime de la BNDJ reposerait, notamment, sur la création d'un code NATINS qui constituerait une source importante d'amélioration du respect des libertés individuelles de l'ensemble des personnes concernées par des informations enregistrées dans l'un des traitements hébergés par la BNDJ. En effet, les traitements judiciaires contiennent des données relatives à des personnes condamnées, mises en cause, des témoins, et des victimes. Un code permettant la discrimination de ces différentes catégories protègerait efficacement les victimes ou les témoins afin que leurs données ne puissent pas faire l'objet d'une extraction lors de la consultation de ces traitements pour y rechercher des personnes ayant des antécédents judiciaires.

1228. Conclusion de la section 2 : la proposition d'un régime pour la BNDJ. – Outre le code NATINS, la proposition de créer la BNDJ contiendrait également la création d'un traitement entièrement dédié à la traçabilité de toutes les actions, techniques ou d'intervention sur les données. La création de ce traitement de traçabilité permettrait de régulariser les droits de l'ensemble des personnes intervenants sur les traitements judiciaires. En effet, actuellement, le cadre légal de la protection des données personnelles n'est pas respecté pour ces intervenants. Une gestion performante de la traçabilité est l'un des atouts majeurs portés par la création de la BNDJ, car la possibilité de pouvoir analyser les actions opérées sur les données serait inextricablement associée à l'amélioration des contrôles de l'utilisation et de la mise à jour des informations stockées dans l'ensemble des traitements judiciaires hébergés.

1229. Conclusion du chapitre 2 : la cohérence des traitements judiciaires améliorée par le regroupement des données. – Les traitements judiciaires sont l'ensemble des traitements de données à caractère personnel mis en œuvre par l'Etat et qui sont directement accessibles par les autorités judiciaires en enquête pénale[2153]. La présente étude propose de créer la BNDJ, qui serait une entité informatique destinée à héberger certains traitements judiciaires, qui sont jusque-là éparpillés auprès de structures différentes. Techniquement, la BNDJ permettrait de concilier le maintien d'un principe de séparation entre les différents traitements judiciaires qui seraient hébergés, avec le regroupement de certaines données communes à ces traitements. La mise en commun de ces données serait une source importante d'amélioration de l'efficacité de l'enquête puisque les enquêteurs accèderaient à des informations beaucoup plus fiables en raison d'un mécanisme de mise à jour plus performant. De plus, cette mise à jour plus fiable des informations contribuerait également à améliorer les libertés individuelles des personnes fichées, en leur garantissant notamment qu'ils ne demeurent pas identifiés comme suspect dans une procédure, alors qu'ils ont été ultérieurement mis hors de cause. Pour créer la BNDJ, une proposition de loi[2154] est nécessaire ainsi qu'un projet de décret. Les deux textes correspondants font l'objet des annexes 2 et 4 des présentes.

1230. Conclusion du titre II : la nécessité de regrouper les données des traitements judiciaires. – Les officiers de police judiciaire ont à leur disposition un nombre croissant de traitements de données à caractère personnel, directement accessibles lors des enquêtes pénales. Non seulement, l'extraction de données depuis ces fichiers constitue une investigation numérique à part entière[2155], mais celle-ci prend de plus en plus d'importance dans l'enquête. Dans ce contexte, la crainte de notre société d'un fichage global et massif des citoyens[2156] a engendré une croyance selon laquelle ces traitements de données sont moins dangereux pour les libertés individuelles lorsqu'ils sont physiquement séparés les uns des autres. Or, la séparation physique des traitements judiciaires induit un cloisonnement des données contenues dans chacun d'entre eux, ce qui nuit à la fois à l'efficacité de l'enquête et aux droits des personnes fichées. D'une part,

[2153] V. *supra* n°968.
[2154] Au sein de la proposition de loi de l'annexe 2, la BNDJ fait l'objet du chapitre 2 de cette proposition puisque le chapitre premier est consacré aux traitements d'exploitation judiciaire.
[2155] V. *supra* n°155.
[2156] Sur le fichage réalisé au sein des fichiers de police, v. not. LAVRIC Sabrina, *Fichiers de police : publication d'un rapport parlementaire*, Recueil Dalloz, 2009 p.938.

l'éparpillement des traitements et le cloisonnement des données vont à l'encontre de la qualité des informations contenues dans ces fichiers puisqu'ils complexifient leur mise à jour dans le temps. D'autre part, ils neutralisent les possibilités de contrôles qui sont pourtant prévues. Pire, la multiplication des traitements engendre un sentiment d'autonomie chez les gestionnaires de certaines bases, qui résistent parfois aux demandes d'effacement ou de rectification d'informations personnelles. Cette situation est largement relevée et dénoncée par plusieurs rapports, émanant de la CNIL[2157] et de travaux parlementaires[2158]. En conséquence, il est nécessaire de dépasser la peur d'un regroupement de certaines données présentes dans différents traitements judiciaires, en faisant converger les possibilités qui sont offertes par les outils informatiques avec les besoins de séparer des informations aux finalités très différentes. C'est l'objectif de la Base Nationale des Données Judiciaires proposée par les présents travaux.

1231. Conclusion de la seconde partie : la nécessité de regrouper les données des investigations numériques. – Les investigations numériques en procédure pénale sont des actes d'enquête qui permettent d'obtenir des données. Ces dernières en constituent donc la caractéristique commune et leurs confèrent des spécificités, telle que la nécessité de pouvoir mobiliser le « savoir de l'enquête » lors de leur exploitation[2159], ou encore la nécessité d'enchaîner et d'entrelacer les investigations numériques les unes aux autres avec rapidité. Ces spécificités conduisent à proposer une amélioration des investigations numériques en se concentrant sur les données obtenues au travers des actes d'investigations numériques. Cette amélioration consisterait à regrouper les données recueillies ou générées. En premier lieu, pour les investigations numériques intrusives, le regroupement des données consisterait à dissocier l'obtention des données au travers des différentes investigations numériques, avec leur analyse qui pourrait se faire au sein du Traitement d'Exploitation Judiciaire (TEJ). Ainsi, l'ensemble des données obtenues

[2157] *Op. cit.* p.35 CNIL, *Conclusions du contrôle du système de traitement des infractions constatées (STIC)*, Rapport remis au Premier ministre le 20 janvier 2009.
Op. cit. p.35 CNIL, *Conclusions du contrôle des fichiers d'antécédents du ministère de l'intérieur.* Rapport adopté en séance plénière le 13 juin 2013.
[2158] *Op. cit.* p.35 BATHO Delphine et BENISTI Jacques-Alain, *rapport d'information sur les fichiers de police,* Commission des lois constitutionnelles, de la législation et de l'administration générale de la République de l'Assemblée Nationale, enregistré le 24 mars 2009.
Op. cit. p.35 BATHO Delphine et BENISTI Jacques-Alain, *rapport d'information sur la mise en œuvre des conclusions de la mission d'information sur les fichiers de police,* Commission des lois constitutionnelles, de la législation et de l'administration générale de la République de l'Assemblée Nationale, enregistré le 21 décembre 2011.
[2159] V. *supra* n°772.

viendraient alimenter le TEJ au fur et à mesure que les actes d'enquête sont exécutés. L'exploitation conjointe de toutes les données améliorerait potentiellement l'efficacité de leur analyse car la corrélation des informations numériques par les outils informatiques devient de plus en plus performante. En second lieu, les investigations numériques d'extraction de données depuis les traitements judiciaires pourraient être optimisées en créant une Base Nationale des Données Judiciaires (BNDJ) qui permettrait de regrouper certaines données communes à plusieurs traitements judiciaires. Cette mise en commun de données optimiserait la qualité des informations enregistrées et faciliterait leur contrôle.

1232. Les deux regroupements de données proposés pourraient se faire sans chamboulement de la procédure pénale, et amélioreraient conjointement l'efficacité de l'enquête et le respect des droits des personnes concernées par les données personnelles recueillies lors d'une enquête pénale, et parfois conservées.

CONCLUSION

1233. Le dépassement de la présente étude. – Les présents travaux sur « les investigations numériques en procédure pénale » montrent que ce sujet rejoint une réflexion plus vaste, sur les orientations que les autorités publiques prennent dans le domaine de la protection de la société *(I)*.

Afin d'alimenter cette réflexion, des projets scientifiques sur des axes de recherches pluridisciplinaires pourraient, en s'appuyant sur les présents travaux, contribuer à donner un nouvel éclairage à la place et aux modalités de mise en œuvre des techniques numériques au sein de l'enquête pénale *(II)*.

I – Une étude inscrite dans la politique de protection de la société

1234. Un acte de procédure et des données comme résultat. – Il est souvent d'usage de dire qu'en droit, tous les mots comptent. C'est une nouvelle fois le cas avec le sujet de la présente étude qui doit être pris comme un tout indissociable. En effet, les investigations numériques sont des actes de procédure que seules les autorités judiciaires peuvent diligenter, ce qui n'est pas le cas en procédure civile et, notamment, devant les juridictions commerciales, où la charge de la recherche des preuves, dont les preuves numériques, repose sur les parties. Pour autant, lors de l'enquête pénale, les investigations numériques, dont le deuxième critère les définissant est de générer ou de recueillir des données, sont des investigations comme les autres.

1235. Des incohérences dues aux spécificités des données. – Néanmoins, leurs spécificités et les contraintes qui les entourent sont bien réelles et nécessitent des besoins particuliers pour être efficaces. Cependant, en aucun cas ces spécificités et ces contraintes ne justifient que, par exemple, une grande partie du Code de procédure pénale soit remis en question pour les regrouper dans un titre ou un chapitre qui leur serait dédié. D'ailleurs, l'éparpillement des investigations numériques dans le Code ne pose pas, en soit, de problème particulier. En revanche, les difficultés apparaissent avec le manque de cohérence entre les dispositions. Lorsqu'un acte est créé ou modifié, le législateur raisonne sur la finalité qui consiste à collecter une information utile à la manifestation de la vérité, sans se préoccuper que cet élément repose sur des données. Partant, de nombreuses incohérences apparaissent au travers d'actes qui se recoupent lors de leur mise en œuvre technique[2160] et, pire, qui contredisent parfois l'esprit du texte les encadrant[2161]. Ainsi, même si le droit doit rester général dans les principes qu'il pose, le fait de créer des dispositions totalement déconnectées des techniques informatiques aboutit parfois à des aberrations, comme lorsque l'analyse des supports numériques réalisée dans le cadre d'une expertise fait totalement abstraction de la mise en œuvre d'un traitement automatisé de données à caractère personnel, alors que le régime des logiciels de rapprochement judiciaire, très proches dans le fonctionnement technique, respecte les règles de la protection des données personnelles.

1236. La nécessaire collaboration entre le droit et l'informatique. – Ce travail collaboratif est d'autant plus nécessaire que le pire ennemi du droit n'est pas la technique, de même que les contraintes légales ne sont souvent pas le frein le plus important aux innovations technologiques, mais bien les idées reçues qui sont ancrées dans les mœurs populaires.

[2160] Voir la captation des données informatiques (v. *supra* n°570.) et l'interception de correspondances émises par la voie de communications électroniques (v. *supra* n°528.).
De même, pour ce qui est de la mise en place de dispositifs techniques permettant d'accomplir un acte de surveillance, le législateur a parfois opté pour une autorisation à commettre une infraction (c'est le cas avec la géolocalisation. C. pr. pén. art. 230-34. V. *supra* n°467.) et, pour d'autres actes, pour un régime d'irresponsabilité pénale (l'enquête sous pseudonyme C. pr. pén art. 230-46 : « […] procéder aux actes suivants sans en être pénalement responsables […] ».

[2161] *Ibid.* Les interceptions de correspondances permettent-elles d'intercepter des données techniques transitant sur la ligne écoutée et qui ne sont pas, par définition, des correspondances ?

1237. Le rapprochement des traitements de données accessibles en enquête. – Avec les traitements automatisés de données mis en œuvre par l'Etat et accessibles en enquête pénale, il est d'usage de considérer que le fait d'éparpiller physiquement ces bases de données est une source de protection des libertés individuelles. Non seulement il n'en est rien mais, bien au contraire, la multiplication d'une donnée identique dans des traitements judiciaires séparés nuit fortement à la mise à jour de cette information ainsi qu'à la réalisation de contrôles effectifs et efficaces sur les fichiers de police. Une consolidation de ces différentes données en créant une « Base Nationale des Données Judiciaires[2162] » pourrait être opérée en respectant un principe de séparation des informations sensibles et spécialisées par finalités, tout en permettant la mise en commun et la synchronisation des informations communes. Les mises à jour, le suivi et le contrôle de ces traitements, dont la consultation et la gestion sont, non seulement, des investigations numériques à part entière, mais également le socle premier de toute enquête, s'en trouveraient considérablement améliorés.

1238. L'analyse regroupée des données collectées ou générées au cours des actes d'investigation numérique. – Il existe une autre forme de regroupement de données qui présente un intérêt. Elle consisterait à regrouper les données collectées ou générées au sein des différents actes d'investigation numérique. Ici, l'intérêt est principalement d'optimiser l'efficacité de l'exploitation des données qui sont le fruit des actes d'enquête au sein d'une procédure. En effet, une analyse des données cloisonnées acte par acte est potentiellement moins efficace qu'une exploitation de ces mêmes données regroupées. Une nouvelle fois, le droit et les techniques informatiques doivent travailler avec cohérence pour que l'analyse des informations numériques regroupées ne soit pas une source de danger pour une procédure, en cas d'annulation de l'un des actes ayant conduit à fournir une partie de ces données regroupées. Des outils techniques permettraient de garantir une traçabilité complète des corrélations qui sont déduites de l'analyse de ces données, avec leur provenance. Ainsi, en aucun cas, il ne s'agit de proposer la création d'une sorte de pot commun dans lequel les données seraient enregistrées sans se poser de question, puis analysées de manière artisanale. Créer la possibilité d'analyser les données créées et générées au sein d'un même dossier pourrait se faire facilement, sans chamboulement de la procédure, en transformant les logiciels de rapprochement

[2162] V. *supra* n°1068.

judiciaire en un « traitement d'exploitation judiciaire[2163] » des données. La finalité initiale des logiciels de rapprochement judiciaire a été totalement bridée par une décision du Conseil constitutionnel[2164]. Cette limitation concourt à un faire une base adaptée à l'évolution vers un outil permettant l'analyse regroupée des données.

1239. Un meilleur positionnement de l'intervention des experts en informatique. – Pour autant, créer cette possibilité ne suffit pas, et impose de s'intéresser à la saisie de certaines données ou supports numériques en amont de leur analyse. En effet, ces derniers ne peuvent être analysés que par des experts dès lors qu'ils ont été saisis en perquisition. Cette restriction se heurte frontalement aux spécificités des investigations numériques. Celles-ci diffèrent d'autres expertises technologiques en ceci que l'analyse des données contenues sur un support ne peut être réellement efficace que si elle est imbriquée ou conjointe à d'autres investigations numériques que seuls des officiers de police judiciaire peuvent effectuer[2165]. Au demeurant, les enquêteurs contournent le recours aux experts dès qu'ils le peuvent. Les autorités publiques ont conscience de cette situation puisqu'il a été introduit dans le Code de procédure pénale des dispositions permettant aux enquêteurs d'analyser les supports mis sous scellés lors d'une perquisition en toute licéité[2166]. Il suffirait de modifier l'article 60-3 pour que l'analyse de toutes les données puissent se dérouler avec fluidité et efficacité, tout en préservant le contenu du scellé d'origine qui pourrait ainsi être expertisé en cas de contestation de l'une des parties.

1240. Ce changement de fonctionnement conduit à s'interroger sur le rôle des experts judiciaires en informatique. Très loin de devenir inutiles, leur intervention devrait être repositionnée sur l'apport de savoirs spécifiques et particuliers que ne peuvent pas avoir les enquêteurs. Leur valeur ajoutée serait valorisée au travers d'un travail collaboratif avec les officiers de police judiciaire qui pilotent l'enquête, aussi bien pour préparer une intervention en amont d'une perquisition par exemple, qu'en aval pour aider les enquêteurs à comprendre les logiciels ou une infrastructure qu'ils ne connaissent pas.

[2163] V. *supra* n°803.

[2164] Cette décision est venue limiter le rapprochement des données à une seule et même procédure. V. *supra* n°819.

[2165] Infiltration numérique, captation de données, etc. V. *supra* n°932.

[2166] C. pr. pén. art. 60-3 : il permet aux enquêteurs de réquisitionner un expert pour cloner le support et ils peuvent ainsi analyser les données ainsi copiées. V. *supra* n°348.
C. pr. pén. art. 157-2 : cet article crée une liste parallèle aux listes d'experts judiciaires, composée d'enquêteurs. V. *supra* n°351.

1241. Un glissement vers une justice administrative. – L'étude des investigations numériques impulse différents changements qui, *in fine*, s'inscrivent dans une problématique bien plus vaste, concernant la protection globale de notre société. Celle-ci inclue directement la place et les moyens de la justice pénale. En fonction des époques, des lois sont interprétées comme plutôt favorables aux libertés individuelles tandis que d'autres sont vues comme liberticides. Depuis 2015, le contexte de menace terroriste permanent qui s'est installé de manière durable, place évidemment le curseur vers la seconde catégorie. Ainsi, pour renforcer la lutte contre des actions souvent individuelles et isolées, donc difficilement détectables intrinsèquement, les autorités publiques ont tenté de trouver des solutions. Le problème récurrent est de gérer une population d'individus « fichés S[2167] » qui sont identifiés comme potentiellement dangereux mais qui, pour autant, n'ont encore commis aucune infraction à ce stade. Il est impératif de pouvoir agir avant qu'ils ne passent à l'acte.

1242. Pour l'heure, la réponse de l'Etat s'est orientée dans deux directions. La première consiste à créer des infractions qui répriment des faits très en amont de la commission d'une infraction nette et franche. On pense ici à la tentative de punir la consultation de sites terroristes, par deux fois retoquée par le Conseil constitutionnel. Le deuxième axe consiste à confier un pouvoir grandissant aux autorités administratives pour mettre sous surveillance, voire pour limiter les déplacements de ces individus. Avec cette façon de procéder, on est clairement dans une orientation, fortement critiquable, qui consiste à prendre des mesures privatives de liberté en amont de toute infraction pénale.

1243. Un nécessaire retour aux bases de l'enquête judiciaire. – Une autre solution pourrait répondre au besoin, bien réel, d'arriver à protéger notre société d'actes terroristes[2168] en interceptant des individus dans cette zone temporelle qui les conduit de « personnes au comportement suspect » à un passage à l'acte. Durant cette période de transition, l'individu prépare son action et, pour cela, a besoin de moyens. Dans toutes les affaires de terrorisme qui se sont produites ces dernières années, l'enquête réalisée *a posteriori* révèle la présence d'armes et d'explosifs au domicile des protagonistes[2169].

[2167] V. *supra* n°667.
[2168] Tout comme, au demeurant, d'autres actes criminels qui nécessitent de la préparation et des moyens matériels et financiers.
[2169] V. les attentats de Carcassonne/Trèbes en mars 2018. Radouane Lakdim, fiché S, s'était équipé d'une arme à feu et d'explosif avant son passage à l'acte.
Le Monde, 23 mars 2018, *Attaques de Carcassonne et Trèbes : ce que l'on sait.*

Autant d'éléments qui tombent sous le coup de sanctions pénales. Ainsi, comme le souligne des spécialistes du renseignement, c'est par un renforcement des enquêtes judiciaires de proximité que peuvent être interceptés ces individus sur le point de passer à l'acte[2170]. Il n'y a pas de « petites enquêtes » et ce sont souvent celles-ci qui vont, selon le vocabulaire employé par les enquêteurs, « faire sortir » des dossiers importants[2171].

1244. Le rôle essentiel des investigations numériques. – Or, c'est précisément au sein de ce renforcement des enquêtes judiciaires de proximité que les investigations numériques ont un rôle prépondérant à jouer et qu'elles peuvent contribuer au succès de la détection d'un individu s'apprêtant à passer à l'acte. La présente étude a démontré à quel point les actes permettant de les mettre en œuvre offrent une grande efficacité potentielle, et ceci de longue date[2172]. Les limitations proviennent beaucoup plus de moyens techniques et humains. Certaines investigations numériques ne sont réellement accessibles qu'à des services spécialisés en raison de l'équipement et des compétences qu'elles nécessitent. Démocratiser ces équipements à l'ensemble des enquêteurs spécialisés du terrain ferait avancer des enquêtes pour des faits de petite délinquance et, grâce aux traitements judiciaires accessibles en enquête pénale, permettrait d'identifier instantanément un individu potentiellement dangereux lorsque son nom apparaîtrait dans l'une de ces enquêtes.

1245. L'augmentation des moyens de la police judiciaire. – Bien évidemment, renforcer l'ensemble des moyens humains et techniques consacrés à la police judiciaire suppose une augmentation des ressources financières dédiées. Or, depuis 2015, les budgets ont incontestablement augmenté pour répondre à la menace terroriste, mais dans les deux directions évoquées précédemment, à savoir orientée vers la police

---

[2170] MEILLAN Eric, *Le renseignement intérieur : pour l'efficacité dans la démocratie,* LexisNexis, Droit pénal n°7-8, juillet 2016, étude 15 : « D'ailleurs, la Police nationale elle-même avec la disparition du maillage territorial systématique des ex-renseignements généraux, et avec la fermeture de nombreux commissariats annexes, bureaux et postes de police, s'est éloignée du terrain […]. La DGSI ne recevra plus autant de « signaux faibles », c'est-à-dire de petits détails sur les comportements que seuls les services de voix publiques, s'ils sont présents quotidiennement sur le terrain, peuvent collecter en permanence. »

[2171] *Ibid.*

[2172] Certains actes d'investigations sont anciens à l'échelle de la généralisation d'Internet et de l'informatisation personnelle, comme la saisie de données informatiques lors de la perquisition qui est prévue depuis 2004 : loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (article 41 qui a introduit la notion de données informatiques dans l'article 56 du C.pr. pén. relatif aux perquisitions).

administrative et le maintien de l'ordre. Il serait sans doute préférable de consacrer cette augmentation aux moyens de la police judiciaire. En effet, privilégier une solution administrative quasi-répressive ne répond qu'à la finalité de lutte contre la radicalisation et le terrorisme, risquant ainsi de laisser la grande criminalité[2173] se développer, car moins surveillée puisque le plus souvent très éloignée des idéologies religieuses.

II – Une étude comme base à des projets pluridisciplinaires

1246. Des outils numériques au service du droit. – Un lien entre des dispositions juridiques proposées au titre des présents travaux et leur mise en œuvre technique a été explicité à plusieurs reprises au sein des pages précédentes. L'objectif est de démontrer que des outils informatiques, parfaitement rodés et maîtrisés, rendent possible l'évolution d'un cadre légal tel qu'il est envisagé. Pour autant, la présente étude n'a pas la prétention de fournir des solutions techniques « clé en main ». Comme cela a été précédemment évoqué[2174], un travail important entre les services de l'Etat compétents et des industriels du numérique doit être réalisé pour aboutir à des solutions techniques adéquates.

1247. Des perspectives scientifiques. – En revanche, les travaux qui précèdent ouvrent d'autres axes de recherche scientifique, à la croisée des disciplines juridique et informatique. On regrettera qu'actuellement, les projets restent trop séparés. A titre d'exemple, le projet « policier 2025[2175] » est un projet technologique sans que des juristes y soient explicitement associés, tandis qu'au sein du projet européen porté par l'université de Liège, ICTCoop[2176], la communauté universitaire n'est composée que de juristes face aux industriels du numériques, parties prenantes du projet.

1248. La perquisition en ligne. – Au terme de nos travaux, un sujet semble pouvoir réunir les deux communautés de manière pertinente. La perquisition en ligne de données géographiquement distantes[2177] se heurte, d'un point de vue légal, à leur localisation en dehors du territoire national. Cette notion de « territorialisation » des données cristallise l'incompréhension entre les juristes et les informaticiens. De nos jours, dans le fort

[2173] Réseaux de prostitution internationaux associés à de la traite d'êtres humains, trafic de drogues, etc.
[2174] V. *supra* n°919.
[2175] « Policier 2025 » est une initiative de l'Etat visant à engager une réflexion scientifique sur les évolutions susceptibles d'optimiser les moyens des agents sur le terrain.
[2176] Cooperation of ICT companies in criminal investigations.
[2177] V. *supra* n°250.

contexte de dématérialisation de notre société, dont la concrétisation technique est l'hébergement des données en mode *Cloud*[2178], un informaticien ne raisonne pas sur l'endroit géographique où est stockée une information, mais sur les droits d'accès, le débit pour y accéder, ou encore les techniques apportant de la sécurité à cette information. Pour lui, que la donnée soit stockée dans une salle serveur à quelques mètres, ou au sein de l'infrastructure d'un prestataire étranger n'est pas une question prioritaire. Or, le législateur a bien intégré cette notion de dématérialisation en créant la perquisition en ligne, mais s'est, en quelque sorte, arrêté au milieu du gué, en laissant subsister une situation ambiguë lorsque les données sont stockées à l'étranger.

1249. Un manque d'homogénéité entre les différents actes portant des investigations numériques a déjà été évoqué : une nouvelle illustration apparaît ici. En effet, alors que les enquêteurs doivent ici se préoccuper de savoir si les données distantes (bien qu'accessibles depuis le site de la perquisition) sont à l'extérieur de notre territoire, l'agent ou le militaire habilité qui procède à une infiltration numérique[2179] peut aller jusqu'à « extraire et acquérir » du contenu numérique mis en ligne au travers de l'espace infiltré, sans se préoccuper de savoir si le serveur hébergeant ce forum ou se site collaboratif est en France ou à l'étranger.

1250. Un nécessaire projet pluridisciplinaire. – Néanmoins, la perquisition est perçue comme un acte beaucoup plus intrusif et il est légitime que toutes les difficultés potentielles quant à la saisie d'informations, en l'occurrence numériques, soient purgées. Ainsi, une problématique technique, mobilisant des compétences en réseaux, sécurité et génie logiciel, consiste à étudier la faisabilité et la modélisation de nouvelles méthodes d'acquisition et de traçabilité des données. L'objectif est de valider un outil informatique permettant de démontrer les conditions d'accès à des données hébergées à l'extérieur du lieu de la perquisition, mais accessibles depuis cet endroit, de tracer le chemin et de copier les données en les plaçant directement dans un scellé numérique. Ces travaux informatiques pourraient servir de base de travail à une réflexion juridique ayant pour finalité de proposer un cadre légal permettant de saisir des données stockées en dehors du

[2178] V. *supra* n°221.
[2179] C. pr. pén. art. 706-87-1, de l'enquête sous pseudonyme. V. *supra* n°468.

territoire national, mais directement[2180] accessibles depuis l'environnement informatique présent dans les locaux objets de la perquisition.

1251. La perspective de nombreux projets. – Cette description de projet n'a pas pour autre prétention que de montrer la pertinence du travail collaboratif entre le juridique et l'informatique. Les investigations numériques en procédure pénale, qui sont des actes ayant pour point en commun de travailler avec des données, sont, pour l'avenir, un terrain qui ne manquera pas de soulever d'autres questions de ce type afin de répondre au besoin grandissant en matière d'exploitation *forensique* de tous les objets numériques qui se généralisent actuellement, et que les délinquants sont susceptibles d'utiliser au même titre qu'une personne *lambda*.

[2180] C'est-à-dire en utilisant les identifiants de la personne ciblée par la perquisition (v. *supra* n°265.) et sans recourir à la moindre technique de contournement des mesures de sécurité pour accéder à d'autres données que celles ainsi accessibles.

ANNEXES

ANNEXE 1

Description et classification des traitements de données judiciaires

Casier judiciaire

Textes de références	➢ *Livre V, titre 8ème du Code de procédure pénale et art. R62 et s.* ➢ *Créé dans sa forme actuelle par la loi n°80-2 du 4 janvier 1980 relative à l'automatisation du casier judiciaire* ➢ *Voir l'arrêté du 22 février 2011 relatif à un traitement automatisé de données à caractère personnel aux fins de gestion des accès au casier judiciaire national qui créé un T.A.D. uniquement pour gérer les accès à l'hébergement du casier*

Classification : traitement automatisé de données…

…de consultation	**X**	…pour la corrélation des données	

Finalité	Il fait foi en matière de condamnation. On retiendra toutefois une finalité administrative importante, notamment au travers des bulletins 2 et 3 (vérification avant admission à des fonctions ou des postes sensibles)
Responsable du traitement	Ministère de la justice

Les données

Alimentation	Personnes objet du trait.	Quelles données ?
…par les greffes des juridictions	Tout le monde (alimentation par le NIR) Personnes morales	➢ Identification ➢ Condamnations pour crime, délit et contravention 5ième classe ➢ Déclaration d'irresponsabilité pénale si assortie d'une hospitalisation d'office ➢ Condamnations par juridictions étrangères si avis en a été donné aux autorités françaises ➢ Décisions disciplinaires prises par autorité administratives lorsqu'elles édictent ou entrainent une incapacité ➢ Redressement judiciaire et faillite personnelle ➢ Mandats d'arrêt ou des peines privatives de libertés
Texte de référence pour la nature des données : C. pr. pén. art. 768 à 774-1		

Destinataires	Le casier est décomposé en trois bulletins et les destinataires en dépendent. ➢ Bulletin n° 1 : que les autorités judiciaires ➢ Bulletin n°2 : Préfet, autorités administratives de l'Etat pour le recrutement (voir liste C. pr. pén. art. R.79) ➢ Bulletin n°3 : par la personne concernée (le plus souvent pour le communiquer dans des dossiers administratifs) **Les bulletins peuvent être envoyés sous forme électronique**
Durée de conservation	Il s'agit plutôt d'un raisonnement basé sur des conditions d'effacement (une variante consiste à annoter avec la mention « prescrite » certaines condamnations)

Traitement d'antécédents judiciaires (TAJ)

Textes de références	➢ *C. pr. pén. art. 230-6 et s. (section 1 du chapitre II relatifs aux fichiers de police judiciaire)* ➢ *C. pr. pén. art. R40-23 et s.* ➢ *Décret n°2001-583 du 5 juillet 2001 pris pour l'application des dispositions du troisième alinéa de l'article 31 de la loi no 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 (STIC)* ➢ *Décret n° 2013-1268 du 27 décembre 2013 portant modification du décret n°2012-652 du 4 mai 2012 relatif au traitement d'antécédents judiciaires* ➢ *Décret n°2017-1217 du 2 août 2017 modifiant le traitement d'antécédents judiciaires*

Classification : traitement automatisé de données…			
…de consultation	**X**	…pour la corrélation des données	

Finalité	Faciliter la constatation des infractions à la loi pénale, le rassemblement des preuves de ces infractions et la recherche de leurs auteurs
Responsable du traitement	Mis en œuvre par la direction générale de la police nationale et la direction générale de la gendarmerie nationale (Ministère de l'intérieur) Mais, traitement sous le contrôle du procureur de la République territorialement compétent Magistrat désigné par le ministère de la justice pour surveiller le respect des mises à jour du fichier

Les données

Alimentation	**Personnes objet du trait.**	**Quelles données ?**
…par les données recueillies lors des procédures établies par la police ou la gendarmerie	➢ personnes, **sans limitation d'âge**, qui sont suspectées par les enquêteurs ➢ **Victimes** (mais, théoriquement, droit d'opposition) ➢ Personnes mortes ou disparues faisant l'objet d'une procédure judiciaire ➢ Personnes morales	➢ Identification ➢ **Profession** ➢ **Signalement et photographies (pas pour les victimes)** ➢ Tout ce qui touche à l'enquête objet de l'alimentation du fichier (faits, modes opératoires, lieux, dates, **données et images**…)
Texte de référence pour la nature des données : C. pr. pén. art. R40-26.		

Destinataires	Personnels désignés à cet effet de la police et de la gendarmerie Agents des douanes Magistrats du parquet et instructeurs Enquêtes administratives (C. sec. int. art.L234-3 et décret n°2017-1217 du 2 août 2017)
Durée de conservation	✓ Normalement 20 ans mais 40 dans certains cas – 15 ans maximum pour les victimes ✓ Effacement immédiat pour les personnes recherchées dès qu'elles ont été retrouvées ✓ Données maintenues en cas de relaxe ou acquittement (une mention est portée dans le fichier) **sauf si le procureur en décide autrement** ✓ Données de traçabilité pour la consultation conservées 5 ans (C. pr. pén. art. R40-30)

Fichier des personnes recherchées

Textes de références	➢ *C. pr. pén. art. 230-19, (section 3 du chapitre II relatifs aux fichiers de police judiciaire) créé par loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure* ➢ *Décret n°2010-569 du 28 mai 2010 relatif au fichier des personnes recherchées*

Classification : traitement automatisé de données…

…de consultation	**X**	…pour la corrélation des données	

Finalité	De faciliter les recherches et les contrôles effectués, dans le cadre de leurs attributions respectives, par la police, la gendarmerie et les douanes
Responsable du traitement	Mis en œuvre par la direction générale de la police nationale et la direction générale de la gendarmerie nationale (Ministère de l'intérieur)

Les données

Alimentation	**Personnes objet du trait.**	**Quelles données ?**
… par police judiciaire et autorité judiciaire …par autorité administrative compétente (exemple : annulation du permis de conduire)	➢ toutes les personnes faisant l'objet d'une « décision de recherche » par une autorité judiciaire ➢ personnes faisant l'objet d'une procédure pour disparition inquiétante ➢ personnes non identifiées ➢ **personnes frappées de peines de substitution (C. pén. art. 131-6) et de mesures particulières ordonnées dans le cadre du contrôle judiciaire (C. pr. pén. art. 138)** ➢ … (article 2 du décret du 28 mai 2010)	➢ Identification ➢ Signalement ➢ **Photographie** ➢ Motif de la recherche ➢ **Conduite à tenir en cas de découverte**
Texte de référence pour la nature des données : C. pr. pén. art. 230-19		

Destinataires	Policiers et des gendarmes habilités (idem pour les agents des douanes) Autorités judiciaires Services administratifs qui gèrent les étrangers sur le territoire Consultation lors des enquêtes administratives (décret n°2017-1219 du 2 août 2017)
Durée de conservation	Jusqu'à ce que la recherche soit terminée ou 3 ans pour les obligations de quitter le territoire **Données de traçabilité pour les agents ou les militaires qui consultent : 5 ans**

<table>
<tr><th colspan="5">Traitement automatisé relatif au contrôle des personnes placées sous surveillance électronique mobile (PSEM)</th></tr>
<tr><td>Textes de références</td><td colspan="4">➢ C. pr. pén. art. R61-12 et s.
➢ Décret n°2016-261 du 3 mars 2016 relatif aux traitements automatisés du contrôle des personnes placées sous surveillance électronique et sous surveillance électronique mobile et modifiant le code de procédure pénale (deuxième partie : Décrets en Conseil d'Etat)</td></tr>
<tr><td colspan="5">Classification : traitement automatisé de données…</td></tr>
<tr><td colspan="2">…de consultation</td><td>X</td><td colspan="2">…pour la corrélation des données</td></tr>
<tr><td>Finalité</td><td colspan="4">Assurer le contrôle à distance, par un centre de surveillance, de la localisation ainsi que du suivi des personnes majeures placées sous surveillance électronique mobile dans les cas prévus aux art. R61-12 du C. pr. pén.</td></tr>
<tr><td>Responsable du traitement</td><td colspan="4">➢ Mis en œuvre par le directeur de l'administration pénitentiaire (Ministère de la justice)
➢ Placé sous le contrôle d'un magistrat du parquet hors hiérarchie (R61-12)</td></tr>
<tr><td colspan="5">Les données</td></tr>
<tr><td>Alimentation</td><td colspan="2">Personnes objet du trait.</td><td colspan="2">Quelles données ?</td></tr>
<tr><td>…dispositif technique, centre de surveillance</td><td colspan="2">➢ Personnes faisant l'objet d'une mesure de sureté (C. pén. art. 131-36-9)
➢ Toutes les personnes placées sous surveillance électronique mobile</td><td colspan="2" rowspan="2">➢ Identification
➢ Photographie
➢ Toutes les données de la condamnation et relatives au placement
➢ Coordonnées de géolocalisation
➢ Alertes si non-respect (notamment zone d'exclusion)
➢ Données de localisation a posteriori</td></tr>
<tr><td colspan="3">Texte de référence pour la nature des données : R61-14</td></tr>
<tr><td>Destinataires</td><td colspan="4">➢ Centre de surveillance
➢ Administration pénitentiaire (sur alerte du centre de surveillance)
➢ En enquête (R61-12)</td></tr>
<tr><td>Durée de conservation</td><td colspan="4">10 ans après la fin de la surveillance (R61-15)</td></tr>
</table>

Fichier automatisé des empreintes digitales

Textes de références	*Décret n°87-249 du 8 avril 1987 relatif au fichier automatisé des empreintes digitales géré par le ministère de l'intérieur modifié par le décret n° 2015-1580 du 2 décembre 2015*

Classification : traitement automatisé de données…

…de consultation	**X**	…pour la corrélation des données	

Finalité	Traces et empreintes digitales et palmaires
Responsable du traitement	Direction centrale de la police judiciaire au ministère de l'intérieur

Les données

Alimentation	**Personnes objet du trait.**	**Quelles données ?**
… lors des enquêtes pour crime ou délit flagrant …en cas de disparition inquiétante	➢ Les suspects ➢ **Les détenus** ➢ Certains étrangers sur notre territoire ➢ Personnes dont les données transmises par des organismes de coopération internationale ➢ Personnes décédées dans certaines conditions (nécessitant identification) **Les victimes ne sont pas dans ce fichier** (sauf celles nécessitant une identification)	➢ Identification. ➢ **Les clichés anthropométriques** ➢ Les données concernant l'affaire à l'origine de la prise ou du relevé d'empreinte ➢ Les données relatives à l'endroit ou aux conditions où des traces papillaires ont été trouvées ➢ L'endroit où se trouvent les fiches physiques de ces relevés de traces
Texte de référence pour la nature des données : articles 3 et 4 du décret du 2 décembre 2015		

Destinataires	Accès très étendu : tous les services d'identification judicaire, le renseignement criminel, toutes les unités de recherche de la gendarmerie, dans le cadre des enquêtes judiciaires ou toutes les procédures nécessitant une identification
Durée de conservation	(attention : changement au 1er mars 2017). 15 ans mais couramment 25 ans. 25 ans pour criminalité organisée. Mais souvent assortie de l'autorisation du procureur pour l'effacement

Fichier national automatisé des empreintes génétiques

Textes de références	➢ *C. pr. pén. art. 706-54 et s.* ➢ *C. pr. pén. art. R53-9 et s.* ➢ *Décret n°2004-470 du 25 mai 2004 modifiant le code de procédure pénale (deuxième partie : Décrets en Conseil d'Etat) et relatif au fichier national automatisé des empreintes génétiques*

Classification : traitement automatisé de données…

…de consultation	**X**	…pour la corrélation des données	

Finalité	Centraliser les empreintes génétiques issues des traces biologiques ainsi que les empreintes génétiques des personnes déclarées coupables ou des suspects des infractions du C. pr. pén. art. 706-55
Responsable du traitement	➢ Mis en œuvre par la direction centrale de la police judiciaire du ministère de l'intérieur ➢ Placé sous le contrôle d'un magistrat du parquet

Les données

Alimentation	**Personnes objet du trait.**	**Quelles données ?**
… par le procureur de la République ou le juge d'instruction compétent	➢ Personnes condamnées pour les infractions listées au C. pr. pén. art. 706-55 ➢ Suspects pour les mêmes infractions sur demande du procureur ou du juge d'instuction ➢ Personnes déclarées irresponsables pénalement mais poursuivies pour les mêmes faits ➢ Personnes condamnées à l'étranger si avis de la juridiction étrangère ➢ Personnes décédées non identifiées faisant l'objet d'une procédure pour disparition	➢ Traces de personnes inconnues recueillies lors des enquêtes pour les infractions du C. pr. pén. art. 706-55 ➢ Toutes les informations relatives à la procédure à l'origine de l'alimentation du fichier ➢ Données techniques relatives au prélèvement ou à la trace Lorsque connu : ➢ Identification
Texte de référence pour la nature des données : C. pr. pén. art. R53-10 et s..		

Destinataires	Uniquement les agents du service spécialisé créé à cet effet (ils consultent et procèdent aux rapprochements qui leur sont demandés par les autorités judiciaires) Traçabilité des consultations
Durée de conservation	40 ans mais des demandes d'effacement peuvent être formulées selon des procédures complexes

Fichier judiciaire national automatisé des auteurs d'infractions sexuelles ou violentes

Textes de références	➢ *C. pr. pén. art. 706-53-1 et s.* ➢ *C. pr. pén. art. R53-8-1 et s.*

Classification : traitement automatisé de données…

…de consultation	**X**	…pour la corrélation des données	

Finalité	➢ Prévenir le renouvellement des infractions mentionnées à l'art. 706-47 du C. pr. pén. **(couvre bien plus que des infractions sexuelles)** et de faciliter l'identification de leurs auteurs ➢ **Pouvoir imposer des obligations aux personnes inscrites** (justifier d'une adresse valide…)
Responsable du traitement	Tenue par le service du casier judiciaire sous l'autorité du ministre de la justice et le contrôle d'un magistrat

Les données

Alimentation	**Personnes objet du trait.**	**Quelles données ?**
…par le procureur de la république ou le juge d'instruction compétent **(enregistrement sans délai)**	➢ Personnes ayant fait l'objet d'une condamnation (même non définitive), d'une mise en examen pour les faits visés au C. pr. pén. art. 706-47 ➢ Idem pour une décision prise par une juridiction étrangère si avis aux autorités françaises	➢ Identification ➢ Toutes les informations relatives à la procédure qui est à l'origine de l'inscription au fichier
Texte de référence pour la nature des données : C. pr. pén. art. R53-8-7		

Destinataires	➢ Autorités judiciaires ➢ Officiers de police judiciaire dans le cadre de procédures décrites au C. pr. pén. art. 706-47 **étendues à d'autres infractions** ➢ Préfet et certaines administrations ➢ … (C. pr. pén. art. 706-53-7 et R53-8-24) ➢ **Accès par système de télécommunication sécurisé**
Durée de conservation	➢ 20 ans mais 30 ans pour les infractions les plus graves ➢ Données de traçabilité des consultations conservées 3 ans

Fichier judiciaire national automatisé des auteurs d'infractions terroristes

Textes de références	➢ *C. pr. pén. art.706-25-3 et s. et R50-30 et s.* ➢ *C. pén. art. 421-1 à 421-6* ➢ *C. séc. int. art. L224-1* ➢ *Décret n°2015-1840 du 29 décembre 2015 modifiant le code de procédure pénale et relatif au fichier judiciaire national automatisé des auteurs d'infractions terroristes*

Classification : traitement automatisé de données…

…de consultation	**X**	…pour la corrélation des données	

Finalité	➢ Prévenir le renouvellement des infractions mentionnées au 706-25-4 C.P.P. ➢ **Pouvoir imposer des obligations aux personnes inscrites** (justifier d'une adresse valide, déplacement à l'étranger…)
Responsable du traitement	Tenue par le service du casier judiciaire sous l'autorité du ministre de la justice et le contrôle d'un magistrat

Les données

Alimentation	**Personnes objet du trait.**	**Quelles données ?**
… par le procureur de la république **(enregistrement sans délai)** ou par le juge d'instruction ou par les agents de police judiciaire ou **par les services du ministère des affaires étrangères** (changement d'adresse ou nouvelles informations)	➢ Personnes ayant fait l'objet d'une condamnation (même non définitive), d'une mise en examen pour les faits visés à l'art. 706-25-4 du C. pr. pén ➢ Personnes ayant fait l'objet d'une déclaration d'irresponsabilité pénale pour ces faits ➢ Idem pour une décision prise par une juridiction étrangère si avis aux autorités françaises	➢ Identification ➢ Toutes les informations relatives à la procédure qui est à l'origine de l'inscription au fichier ➢ Déplacements transfrontaliers ➢ Obligations qui ont été notifiées ➢ …
Texte de référence pour la nature des données : C. pr. pén. art. 706-25-4 et R50-36.		

Destinataires	➢ Autorités judiciaires ➢ Officiers de police judiciaire dans le cadre de procédures décrites aux articles 421-1 à 421-6 du C. pén. ➢ Aux représentants de l'Etat dans le département et à certaines administrations ➢ … (C. pr. pén. art. 706-25-9) **Accès par système de télécommunication sécurisé**
Durée de conservation	➢ 20 ans ou 10 ans s'il s'agit d'un mineur ➢ Données de traçabilité des consultations conservées 3 ans

Répertoire des données à caractère personnel collectées dans le cadre des procédures judiciaires « REDEX »

Textes de références	➢ *C. pr. pén. art. 706-56-2 et R53-21-1 et s. (entrées en vigueur au 1er mars 2018)* ➢ *Décret n°2016-1338 du 7 octobre 2016 modifiant le code de procédure pénale et relatif au répertoire des données collectées dans le cadre d'une procédure judiciaire*

Classification : traitement automatisé de données…			
…de consultation	**X**	…pour la corrélation des données	

Finalité	Faciliter et fiabiliser la connaissance de la personnalité et l'évaluation de la dangerosité des personnes poursuivies ou condamnées pour l'une des infractions pour lesquelles le suivi socio-judiciaire est encouru, et à prévenir le renouvellement de ces infractions
Responsable du traitement	Tenue par le service du casier judiciaire sous l'autorité du ministre de la justice et le contrôle d'un magistrat

Les données

Alimentation	**Personnes objet du trait.**	**Quelles données ?**
… au cours de l'enquête, de l'instruction, lors du jugement, au cours de l'exécution de la peine	➢ Personnes décrites dans la finalité du traitement *(voir C. pr. pén. art. R53-21-2)* ➢ *Personnes condamnées **et poursuivies** au sens des alinéas 10 et 1er de l'article 706-56-2, et celles condamnées pour l'une des infractions pour lesquelles le suivi socio-judiciaire est encouru*	➢ Identification ➢ Résultats des expertises, évaluations et examens psychiatriques, psychologiques et pluridisciplinaires ➢ Données relatives aux poursuites et condamnations, correspondantes
Texte de référence pour la nature des données : C. pr. pén. art. R53-21-2 et s.		

Destinataires	➢ Autorités judiciaires ➢ Membres de la commission pluridisciplinaire des mesures de sûreté ➢ Experts ➢ Personnes chargées d'évaluer la dangerosité de l'individu
Durée de conservation	Maximum 30 ans ou 15 ans si mineur Données de traçabilité pendant 3 ans *(C. pr. pén. art. R53-21-19)*

Traitements automatisés de contrôle des données signalétiques des véhicules

Textes de références	➢ *Arrêté du 18 mai 2009 portant création d'un traitement automatisé de contrôle des données signalétiques des véhicules* ➢ *Voir la similitude avec C. séc. int. art. L233-1 et s.*

Classification : traitement automatisé de données…

…de consultation	**X**	…pour la corrélation des données	

Finalité	Prévenir et réprimer le terrorisme, faciliter la constatation des infractions criminelles ou liées à la criminalité organisée, des infractions de vol et de recel de véhicules volés. Rassembler les preuves de ces infractions et la recherche de leurs auteurs. Préserver l'ordre public.
Responsables du traitement	Directeur général de la police nationale, directeur général de la gendarmerie nationale et le directeur général des douanes et droits indirects.

Les données

Alimentation	**Personnes objet du trait.**	**Quelles données ?**
… par la mise en place de dispositifs automatiques de lecture des plaques d'immatriculation	➢ Indirectement le propriétaire du véhicule car le numéro d'immatriculation du véhicule est enregistré ➢ Les éventuels occupants du véhicule	➢ Photo du véhicules <u>et de ses éventuels occupants</u> ➢ Date et heure ➢ Coord. GPS ➢ Si rapprochement positif avec un autre traitement, le motif de signalement et la conduite à tenir pour le véhicule concerné
Texte de référence pour la nature des données : arrêté du 18 mai 2009 art. 3.		

Destinataires	➢ Agents des services de police et gendarmerie ainsi que des douanes habilités
Durée de conservation	Entre 8 jours et 1 mois si aucun rapprochement La durée d'une éventuelle procédure judiciaire si rapprochement positif avec un autre traitement

<table>
<tr><th colspan="4">Fichier des objets et des véhicules signalés (FOVeS)</th></tr>
<tr><td>Texte de référence</td><td colspan="3">➢ Arrêté du 17 mars 2014 portant autorisation à titre expérimental d'un traitement automatisé de données à caractère personnel dénommé « Fichier des objets et des véhicules signalés » (FOVeS)</td></tr>
<tr><td colspan="4">Classification : traitement automatisé de données…</td></tr>
<tr><td>…de consultation</td><td>X</td><td>…pour la corrélation des données</td><td></td></tr>
<tr><td>Finalité</td><td colspan="3">Faciliter les recherches de la police et de la gendarmerie ainsi que celles effectuées par les agents des douanes habilités […] à l'occasion des contrôles relevant de leurs attributions pour la découverte, la restitution et la surveillance des véhicules et des objets signalés volés.</td></tr>
<tr><td>Responsables du traitement</td><td colspan="3">Directeur général de la police nationale et directeur général de la gendarmerie nationale.</td></tr>
<tr><td colspan="4">Les données</td></tr>
<tr><td>Alimentation</td><td>Personnes objet du trait.</td><td colspan="2">Quelles données ?</td></tr>
<tr><td>… par les procédures judiciaires diligentées pour des faits de vol,
…par les mesures de surveillance,
…par les déclarations de perte
…par les décisions d'invalidation de documents prononcées par les autorités administratives.</td><td>➢ Toutes les personnes dont le nom figure dans les données servant à alimenter le traitement.</td><td colspan="2">➢ Photos,
➢ Contexte de l'affaire,
➢ Conduite à tenir
➢ … voir annexe de l'arrêté

➢ Distinction en fonction de l'origine de l'alimentation.</td></tr>
<tr><td colspan="2">Texte de référence pour la nature des données : l'annexe de l'arrêté du 17 mars 2014.</td><td colspan="2"></td></tr>
<tr><td>Destinataires</td><td colspan="3">➢ Agents des services de police et gendarmerie ainsi que des douanes habilités
➢ Certaines autorités administratives
➢ Les autorités judiciaires</td></tr>
<tr><td>Durée de conservation</td><td colspan="3">Entre 5 et 50 ans (armes) – 6 mois pour les mesures de surveillance
Données de traçabilité pendant 5 ans</td></tr>
</table>

Plate-forme nationale des interceptions judiciaires (PNIJ)

Textes de références	➢ *C. pr. pén. art. 230-45 et R40-42 et s.* ➢ *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 »* ➢ *Délibération n°2014-009 du 16 janvier 2014 portant avis sur [...] un traitement de données à caractère personnel dénommé PNIJ* ➢ *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*

Classification : traitement automatisé de données…

…de consultation	**X**	…pour la corrélation des données	

Finalité	Faciliter la constatation des infractions à la loi pénale, le rassemblement des preuves de ces infractions et la recherche de leurs auteurs
Responsable du traitement	Placé sous la responsabilité du secrétaire général du ministère de la justice Compétence de l'ANTEJ pour la gestion des données collectées (v. art.2 du décret du 24 avril 2017)

Les données

Alimentation	**Personnes objet du trait.**	**Quelles données ?**
… PNIJ qui se positionne en interface avec les opérateurs de télécommunications	➢ Personnes faisant l'objet d'une mesure d'interception de correspondance, de géolocalisation	➢ Contenu des communications électroniques interceptées ➢ Identification ➢ Données techniques inhérentes à l'interception ➢ Données de facturation ➢ Données de géolocalisation ➢ Données liées aux faits ➢ **Données politiques ou religieuses...**
Texte de référence pour la nature des données : C. pr. pén. art. R40-43, R40-44, R40-46		

Destinataires	Magistrats, officiers de police judiciaire… C. pr. pén. art. R40-47
Durée de conservation	Conservation jusqu'à l'expiration du délai de prescription de l'action publique (moyennant une mise sous scellé des enregistrements).

<table>
<tr><th colspan="5">Traitements de données informatiques captées</th></tr>
<tr><td>Textes de références</td><td colspan="4">➢ C. pr. pén. art. 706-102-1 et s.
➢ Décret n°2015-1700 du 18 décembre 2015 relatif à la mise en œuvre de traitements de données informatiques captées en application de l'article 706-102-1 du code de procédure pénale</td></tr>
<tr><td colspan="5">Classification : traitement automatisé de données…</td></tr>
<tr><td colspan="2">…de consultation</td><td>X</td><td>…pour la corrélation des données</td><td></td></tr>
<tr><td>Finalité</td><td colspan="4">Permettre la constatation des crimes et délits entrant dans le champ d'application des articles 706-73 et 706-73-1 de ce code, le rassemblement des preuves de ces infractions et l'identification de leurs auteurs,</td></tr>
<tr><td>Responsable du traitement</td><td colspan="4">Ministre de l'intérieur (direction générale de la police nationale, direction générale de la gendarmerie nationale, direction générale de la sécurité intérieure et préfecture de police) et le ministre des finances et des comptes publics (direction générale des douanes et droits indirects)</td></tr>
<tr><td colspan="5">Les données</td></tr>
<tr><td>Alimentation</td><td colspan="2">Personnes objet du trait.</td><td colspan="2">Quelles données ?</td></tr>
<tr><td>… collecte, enregistrement et conservation de données issues des dispositifs techniques de captation</td><td colspan="2">➢ Personnes faisant l’objet de la mesure de surveillance</td><td colspan="2" rowspan="2">➢ L’ensemble des données captées

Très flou car l’article 8 du décret renvoi à un dossier technique de présentation du logiciel</td></tr>
<tr><td colspan="3">Texte de référence pour la nature des données : article 2 du décret du 18 décembre 2015</td></tr>
<tr><td>Destinataires</td><td colspan="4">Magistrats accèdent à l’ensemble des données
Officiers et agents de police judiciaire ainsi que les agents des douanes et des services fiscaux : accès plus encadré</td></tr>
<tr><td>Durée de conservation</td><td colspan="4">Jusqu’à la clôture des investigations (alors placées sous scellés fermés et effacés)
Données de traçabilité des consultations conservées 6 ans</td></tr>
</table>

Traitement de données à caractère personnel API-PNR France			
Textes de références	➢ *C. séc. int. art. L232-1 à L232-8* ➢ *C. séc. int. art. R232-12 à R232-18* ➢ *Délibération n° 2014-308 du 17 juillet 2014 portant avis sur un projet de décret relatif à la création d'un traitement de données à caractère personnel dénommé « système API-PNR France » pris pour l'application de l'article L. 232-7 du code de la sécurité intérieure et fixant les modalités de transmission au service à compétence nationale « Unité Information Passagers » des données relatives aux passagers par les transporteurs aériens* ➢ *Décret n°2017-1467 du 13 octobre 2017 modifiant le code de procédure pénale (partie réglementaire - Décrets simples)*		
Classification : traitement automatisé de données…			
…de consultation	**X**	…pour la corrélation des données	
Finalité	Suivi des voyageurs via le transport aérien transfrontalier et sur le territoire national		
Responsable du traitement	➢ Mis en œuvre par les ministres de l'intérieur, de la défense, chargé des transports et chargé des douanes ➢ Exploité par le service dénommé « Unité Information Passagers « (UIP) rattaché au ministre chargé des douanes		
Les données			
Alimentation	**Personnes objet du trait.**	**Quelles données ?**	
… l'Unité Information Passagers est responsable de la collecte des données des passagers	Les données à caractère personnel et informations relatives aux passagers aériens transmises par les transporteurs aériens	Très vaste et très complet : v. C. séc. int. art. R232-14	
Texte de référence pour la nature des données : C. séc. int. art. R232-14.			
Destinataires	Seuls les personnels affectés au sein de l'Unité Information Passagers ont un accès direct aux données mais ils répondent aux requêtes, notamment, des « directions interrégionales et régionales de la direction centrale de la police judiciaire » et des « sections de recherches de la gendarmerie nationale » dans le cadre des infractions de criminalité organisée c'est-à-dire bien au-delà du terrorisme (finalité première). V. C. séc. int. art. 232-15		
Durée de conservation	5 ans – 5 ans aussi pour la traçabilité de consultation		

Système d'Information Schengen (SIS) :
N-SIS
SIRENE - Gestion électronique de documents (GED)

Textes de références	➢ *C. séc. int. art. R231-1 et s.*

Classification : traitement automatisé de données…

…de consultation	**X**	…pour la corrélation des données	

Finalité	➢ N-SIS : centralisation d'informations concernant les personnes et objets recherchés par les autorités administratives et judiciaires des Etats parties à l'accord de Schengen, afin de permettre aux autorités désignées par ces Etats de mettre en œuvre des conduites à tenir relatives aux personnes et objets recherchés ➢ GED : éléments de signalement, et informations concernant des signes physiques qui peuvent faire apparaître, directement ou indirectement, des données relevant du I de l'article 8 de la loi Informatique et Libertés, lorsque celles-ci constituent des éléments déterminants pour l'identification des personnes qui sont enregistrées N-SIS
Responsable du traitement	Direction générale de la police nationale (Ministère de l'intérieur)

Les données

Alimentation	**Personnes objet du trait.**	**Quelles données ?**
… par toutes les autorités désignées dans chaque état membre	➢ Les personnes recherchées pour arrestation aux fins d'extradition ; ➢ Les étrangers signalés aux fins de non-admission à la suite d'une décision administrative ou judiciaire ; ➢ Les personnes disparues et les personnes qui, dans l'intérêt de leur propre protection ou pour la prévention de menaces, doivent être placées provisoirement en sécurité ; ➢ Les personnes recherchées par l'autorité judiciaire dans le cadre d'une procédure pénale ; ➢ Les personnes recherchées par l'autorité judiciaire pour la notification ou l'exécution d'une décision pénale.	➢ Identification ➢ Signes particuliers ➢ Conduite à adopter en cas de découverte Pour les objets : caractéristiques propres au type d'objet Pour GED : voir la finalité du traitement de données
Texte de référence pour la nature des données : C. séc. int. art. R-231-9 et R231-10		

Destinataires	Notamment : **les autorités judiciaires** et les fonctionnaires de la police nationale et les militaires de la gendarmerie nationale dûment habilités qui agissent dans le cadre de leur mission générale de police administrative et **de police judiciaire** (v. C. séc. int. art. R231-11)
Durée de conservation	Non précisé

Traitement de données à caractère personnel dénommé « Enquêtes administratives liées à la sécurité publique » *(EASP)*

Textes de références	➢ *C. séc. int. art. R236-1 et s.* ➢ *Décret n°2009-1250 du 16 octobre 2009 portant création d'un traitement automatisé de données à caractère personnel relatif aux enquêtes administratives liées à la sécurité publique* ➢ *CNIL : Délibération 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*

Classification : traitement automatisé de données…

…de consultation	**X**	…pour la corrélation des données	

Finalité	Faciliter la réalisation d'enquêtes administratives pour les personnes appelées à occuper certaines fonctions dans le domaine de la sécurité ou en vue d'obtenir la nationalité française.
Responsable du traitement	Direction centrale de la sécurité publique et préfecture de police (ministre de l'intérieur)

Les données

Alimentation	**Personnes objet du trait.**	**Quelles données ?**
… service chargé de la mise en œuvre	Personnes appelées à occuper certaines fonctions dans le domaine de la sécurité. Personnes demandant la nationalité française.	➢ Motif de l'enquête ➢ Identification ➢ **Photographies** ➢ Titres d'identité ➢ **Le rapport de l'enquête administrative, contenant les éléments permettant de déterminer si le comportement de la personne concernée n'est pas incompatible avec l'exercice des fonctions ou des missions envisagées, compte tenu de leur nature.**
Texte de référence pour la nature des données : C. séc. int. art. R236-2		

Destinataires	Notamment : « dans la limite du besoin d'en connaître, tout autre membre d'une unité de la gendarmerie nationale ou agent d'un service de la police nationale » (voir C. séc. int. art. R236-6)
Durée de conservation	5 ans maximum à compter de leur enregistrement – 5 ans la traçabilité de consultation

Traitement de données à caractère personnel dénommé « Prévention des atteintes à la sécurité publique » *(PASP)*

Textes de références	➢ *C. séc. int. art. R236-11 et s.* ➢ *Décret n°2009-1249 du 16 octobre 2009 portant création d'un traitement de données à caractère personnel relatif à la prévention des atteintes à la sécurité publique* ➢ *CNIL : Délibération n°2009-355 du 11 juin 2009 portant avis sur un projet de décret en Conseil d'Etat portant création de l'application relative à la prévention des atteintes à la sécurité publique*

Classification : traitement automatisé de données…

…de consultation	**X**	…pour la corrélation des données	

Finalité	Recueillir, conserver et **analyser** les informations qui concernent des personnes dont l'activité individuelle ou collective indique qu'elles peuvent porter atteinte à la sécurité publique. Ce traitement a notamment pour finalité de recueillir, de conserver et d'analyser les informations qui concernent les personnes susceptibles d'être impliquées dans des actions de violence collectives, en particulier en milieu urbain ou à l'occasion de manifestations sportives.
Responsable du traitement	Direction générale de la police nationale (ministre de l'intérieur)

Les données

Alimentation	**Personnes objet du trait.**	**Quelles données ?**
… service chargé de la mise en œuvre	Personnes dont l'activité individuelle ou collective indique qu'elles peuvent porter atteinte à la sécurité publique, notamment en étant impliqué dans des actions terroristes (ajouté par le Décret n°2017-1216 du 2 août 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)	➢ Identification ➢ **Photographies** ➢ **Agissements susceptibles de recevoir une qualification pénale** ➢ Données religieuses ou politiques ➢ Immatriculation des véhicules ➢ Informations patrimoniales ➢ **Personnes entretenant ou ayant entretenu des relations directes et non fortuites avec l'intéressé.**
Texte de référence pour la nature des données : C. séc. int. art. R236-12		

Destinataires	Notamment : « dans la limite du besoin d'en connaître, tout autre membre d'une unité de la gendarmerie nationale ou agent d'un service de la police nationale » (voir C. séc. int. art. R236-16 : liste étendue par le décret du 2 août 2017)
Durée de conservation	3 ans maximum après l'intervention du dernier événement de nature à faire apparaître un risque d'atteinte à la sécurité publique ayant donné lieu à un enregistrement – 5 ans la traçabilité de consultation

Traitement de données à caractère personnel dénommé « Gestion de l'information et prévention des atteintes à la sécurité publique »

Textes de références	➢ *C. séc. int. art. R236-21 et s.*

Classification : traitement automatisé de données…

…de consultation	**X**	…pour la corrélation des données	

Finalité	Recueillir, conserver et **analyser** les informations qui concernent des personnes dont l'activité individuelle ou collective indique qu'elles peuvent porter atteinte à la sécurité publique. Ce traitement a notamment pour finalité de recueillir, de conserver et d'analyser les informations qui concernent les personnes susceptibles d'être impliquées dans des actions de violence collectives, en particulier en milieu urbain ou à l'occasion de manifestations sportives.
Responsable du traitement	Direction générale de la gendarmerie nationale (ministre de l'intérieur)

Les données

Alimentation	**Personnes objet du trait.**	**Quelles données ?**
… service chargé de la mise en œuvre	Personnes dont l'activité individuelle ou collective indique qu'elles peuvent porter atteinte à la sécurité publique	➢ Identification ➢ **Photographies** ➢ **Agissements susceptibles de recevoir une qualification pénale** ➢ Données religieuses ou politiques ➢ Immatriculation des véhicules ➢ Informations patrimoniales ➢ **Personnes entretenant ou ayant entretenu des relations directes et non fortuites avec l'intéressé**
Texte de référence pour la nature des données : C. séc. int. art. R236-22.		

Destinataires	Notamment : « dans la limite du besoin d'en connaître, tout autre membre d'une unité de la gendarmerie nationale ou agent d'un service de la police nationale » (voir C. séc. int. art. R236-26)
Durée de conservation	3 ans maximum après l'intervention du dernier événement de nature à faire apparaître un risque d'atteinte à la sécurité publique ayant donné lieu à un enregistrement – 5 ans la traçabilité de consultation

Traitement de données à caractère personnel dénommé « Sécurisation des interventions et demandes particulières de protection »			
Textes de références	➢ *C. séc. int. art. R236-38 et s.* ➢ *Décret n°2011-342 du 29 mars 2011 portant création d'un traitement de données à caractère personnel relatif à la sécurisation des interventions et demandes particulières de protection*		
Classification : traitement automatisé de données…			
…de consultation	**X**	…pour la corrélation des données	
Finalité	Collecter des données destinées à une gestion des interventions des forces de gendarmerie adaptée soit aux personnes dont la dangerosité ou l'agressivité, à travers des manifestations de violence physique ou verbale, déjà constatée lors d'une précédente intervention,		
Responsable du traitement	Direction générale de la gendarmerie nationale (ministre de l'intérieur)		

Les données		
Alimentation	**Personnes objet du trait.**	**Quelles données ?**
… services de gendarmerie	➢ Personnes demandant une intervention ➢ Personnes se trouvant dans une situation de vulnérabilité particulière.	➢ Identification ➢ **Photographies** ➢ Données religieuses ou politiques ➢ Nombre de personnes au domicile ➢ **Détention d'arme ou de chien de première ou seconde catégorie**
Texte de référence pour la nature des données : C. séc. int. art. R236-39 et R236-4		
Destinataires	Gendarmes et « dans la limite du besoin d'en connaître, tout autre membre d'une unité de la gendarmerie nationale ou agent d'un service de la police nationale » (voir C. séc. int. art. R236-43)	
Durée de conservation	10 ans maximum – 3 ans la traçabilité de gestion du traitement	

Logiciels de rapprochement judiciaire

Textes de références	➢ *C. pr. pén. art. 230-20 et s.* ➢ *C. pr. pén. art. R40-39 et s.* ➢ *Décret n°2012-687 du 7 mai 2012 relatif à la mise en œuvre de logiciels de rapprochement judiciaire à des fins d'analyse criminelle* ➢ *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*

Classification : traitement automatisé de données…			
…de consultation		…pour la corrélation des données	**X**

Finalité	L'exploitation et le rapprochement d'informations sur les modes opératoires réunies au cours d'une même enquête par les services de la police nationale et de la gendarmerie
Responsable du traitement	Direction de la gendarmerie et direction de la police, préfecture de police (ministère de l'intérieur) Un magistrat est chargé du contrôle (désigné par ministre de la justice)

Les données

Alimentation	**Personnes objet du trait.**	**Quelles données ?**
… données recueillies lors des enquêtes ou des investigations exécutées sur commission rogatoire ainsi que lors des procédures pour recherche des causes de la mort	➢ Les personnes citées dans les procédures à l'origine de l'alimentation du fichier ➢ **ATTENTION : exploitation du fichier sur mots clés, mais utilisation des données nominatives encadrée**	➢ Tout ce qui touche au mode opératoire ➢ **Données sensibles au sens de la loi Informatique et Liberté** Très flou car l'article 6 du décret renvoi à un dossier technique de présentation du logiciel
Texte de référence pour la nature des données : C. pr. pén. art. R230-21 et R230-22		

Destinataires	✓ Services de police et gendarmerie ✓ Magistrats du parquet, de l'instruction ✓ **Utilisation exclue pour les enquêtes administratives**
Durée de conservation	Données nominatives révélées par le logiciel sont effacées à la clôture de l'enquête ou au plus tard dans un délai de 3 ans Données de traçabilité des consultations conservées 5 ans

Fichiers d'analyse sérielle

Textes de références	➢ *C. pr. pén. art. 230-12 et s.* ➢ *C. pr. pén. art. R40-35 et s.* ➢ *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 »* ➢ *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*

Classification : traitement automatisé de données…			
…de consultation		…pour la corrélation des données	**X**

Finalité	Rassembler les preuves et 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
Responsable du traitement	Direction de la gendarmerie et direction de la police, préfecture de police (ministère de l'intérieur)

Les données

Alimentation	**Personnes objet du trait.**	**Quelles données ?**
… données recueillies lors des enquêtes ou des investigations exécutées sur commission rogatoire et concernant toute infraction punie d'au moins cinq ans d'emprisonnement ainsi que lors des procédures pour recherche des causes de la mort	➢ Suspects ➢ **Personnes susceptibles de fournir des renseignements** ➢ **Victimes**	**Distinction entre personnes mises en cause, victimes et les témoins** ✓ Identification ✓ Photographies ✓ Images et vidéos en lien avec l'enquête ✓ Mode de transport ✓ **Liens avec les faits** **Moins de données pour les victimes et les témoins** Très flou car l'article 7 du décret renvoi à un dossier technique de présentation du logiciel
Texte de référence pour la nature des données : annexe du décret du 22 novembre 2013		

Destinataires	Accès directs uniquement pour des policiers ou gendarmes habilités Via une demande aux agents ou militaires habilités : ✓ Services de police et gendarmerie ✓ Magistrats du parquet, de l'instruction ✓ **Utilisation exclue pour les enquêtes administratives**
Durée de conservation	15 ans pour les délits et 20 ans pour les crimes Données de traçabilité des consultations conservées 5 ans

ANNEXE 2

Proposition de loi visant à améliorer l'efficacité et à renforcer les garanties des traitements de données en procédure pénale

> CHAPITRE PREMIER : DISPOSITIONS RELATIVES AUX TRAITEMENTS D'EXPLOITATION JUDICIAIRE

Article 1

L'intitulé du chapitre III du titre IV du livre Ier du Code de procédure pénale, est remplacé par : « Des traitements d'exploitation judiciaire ».

Article 2

A l'article 230-20 du même Code, après la deuxième occurrence du mot « judicaire, » la fin de la phrase est remplacée par : « des traitements destinés à exploiter les données et à faciliter le rapprochement d'informations sur les modes opératoires, réunies par ces services au cours : »

Article 3

L'article 230-21 du même Code est ainsi modifié :

- Au premier alinéa, les mots « par les logiciels » sont remplacés par « au sein des traitements », et avant le mot « pièces » est inséré « données, ».
- Le deuxième alinéa est supprimé.

Article 4

Le premier alinéa de l'article 230-22 du même Code est ainsi modifié :

- Le mot « Les » est remplacé par « L'ensemble des ».
- Les mots « éventuellement révélées par l'exploitation » sont remplacés par « exploitées et rapprochées lors ».
- Après la deuxième occurrence du mot « enquête », la fin de la phrase est remplacée par « selon des modalités définies par décret. »

Le deuxième alinéa de l'article 230-22 du même Code est ainsi modifié :

- Le mot « Les » est remplacé par « L'ensemble des ».
- Les mots « éventuellement révélées par l'exploitation » sont remplacés par « exploitées et rapprochées lors ».

Article 5

Au premier alinéa de l'article 230-23 du même Code, après le mot « compétent », la fin de la phrase est supprimée.

Au deuxième alinéa du même article, le mot « logiciels » est remplacé par « traitements ».

Article 6

Au premier alinéa de l'article 230-24 du même Code, le mot « logiciels » est remplacé par « traitements » et les mots « et de s'assurer de la mise à jour des données » sont supprimés.

Au troisième alinéa du même article, le mot « logiciels » est remplacé par « traitements ».

Article 7

Au premier alinéa de l'article 230-25, ainsi qu'à l'article 230-26 du même Code, le mot « logiciels » est remplacé par « traitements ».

Au premier alinéa de l'article 230-27, le mot « logiciels » est remplacé par « traitements », et les mots « logiciel » est remplacé par « des traitements ».

Article 8

L'article 60-3 du même Code est supprimé et ainsi rétablie :

« Lorsqu'ont été placés sous scellés des objets qui sont le support de données informatiques, les agents ou militaires habilités et désignés au 1° de l'article 230-25 du présent code, peuvent, sur autorisation du procureur de la République, procéder à l'ouverture des scellés pour réaliser une ou plusieurs copies de ces données sans porter atteinte à leur intégrité, afin de permettre leur exploitation dans les conditions prévues à l'article 230-20. Les scellés sont reconstitués lorsque les opérations de copie sont terminées.

L'autorisation du procureur de la République fait l'objet d'une mention dans la procédure.

La copie des données donne lieu à l'établissement d'un rapport joint à la procédure qui fait mention des opérations effectuées et qui dresse l'inventaire des scellés exploités. »

Article 9

L'article 77-1-3 du même Code est ainsi modifié : « Le procureur de la République peut autoriser la copie des données prévue à l'article 60-3. »

L'article 99-5 est ainsi modifié : « Pour les nécessités de l'exécution de la commission rogatoire, le juge d'instruction peut autoriser la copie des données prévue à l'article 60-3. L'autorisation du juge d'instruction fait l'objet d'une mention dans la procédure.

Les dispositions du sixième alinéa de l'article 97 ne sont pas applicables. »

> CHAPITRE 2 : DISPOSITIONS RELATIVES A LA BASE NATIONALE DES DONNEES JUDICIAIRES

Article 10

Le titre IV du livre Ier du Code de procédure pénale, est complété par un chapitre VIII ainsi rédigé :

Chapitre VIII

De la base nationale des données judiciaires

Art. 230-47. – Afin de faciliter la mise à jour et le contrôle des informations enregistrées dans les traitements automatisés de données à caractère personnel dont la liste est précisée par décret, il est créé une base nationale des données judiciaires tenue par le service du casier judiciaire sous l'autorité du ministre de la justice.

Un code unique est associé aux personnes faisant l'objet d'un enregistrement dans l'un ou plusieurs de ces traitements, aux fins de déterminer si elles y sont présentes :

a° en qualité de personnes mises en cause, condamnées ou recherchées,

b° en qualité de témoins,

c° en qualité de victimes.

Un quatrième code est affecté aux agents, militaires et autre personnel habilité à accéder et opérer sur les données, dans le respect de la traçabilité prévue à l'article 230-50.

Art. 230-48. – La base nationale des données judiciaires est directement accessible, par l'intermédiaire d'un système de télécommunication sécurisé :

1° A l'ensemble des personnes prévues par les dispositions spécifiques à chaque traitement hébergé. Les conditions d'alimentation et de consultation prévues pour chaque traitement s'appliquent strictement.

2° A la personne qualifiée ainsi qu'aux membres du comité prévus à l'article 230-51, pour le strict exercice de leur mission.

Art. 230-49. – Une interconnexion technique au sens du 3° du I de l'article 33 de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés est mise en œuvre afin de garantir l'identité des informations saisies entre les différents traitements de données à caractère personnel hébergés.

La même interconnexion technique peut être mise en œuvre avec un autre traitement de données, afin de permettre l'identité des informations présentes dans la base nationale de données judiciaires avec celles de ce traitement.

Art. 230-50. - Toute mise à jour ou tout effacement des données personnelles stockées dans l'un des traitements hébergés, ordonné par l'autorité judiciaire compétente ou légalement prévue, est répercuté dans l'ensemble des autres traitements hébergés.

Art. 230-51. - Les consultations ainsi que toutes les actions réalisées sur les données, font l'objet d'un enregistrement permettant une traçabilité complète. Les modalités de cette traçabilité sont précisées par décret.

Art. 230-52. - La base nationale des données judiciaires est placée sous le contrôle d'une personnalité qualifiée, assistée par un comité, selon des conditions définies par décret.

Art. 230-53. - Un décret en Conseil d'Etat, pris après avis de la Commission nationale de l'informatique et des libertés, fixe les modalités d'application du présent chapitre. Il précise notamment la liste des traitements de données à caractère personnel hébergés par la base nationale de données judiciaires en application de l'article 230-46.

Article 11

Au premier alinéa de l'article 230-6 du Code de procédure pénale, après le mot « personnel » est inséré « hébergés par la base nationale des données judiciaires ».

A la cinquième phrase du premier alinéa de l'article 230-8, après le mot « concernée », est inséré « ainsi que la personnalité en charge du contrôle de la base nationale des données judiciaires prévue à l'article 230-52. »

Article 12

Au premier alinéa de l'article 48-1 du même code, après le mot « automatisée » est inséré « hébergée par la base nationale des données judiciaires ».

Article 13

L'article 706-54 du même code est ainsi modifié :

- Le deuxième alinéa est complété par : « Lorsque le procureur de la République n'a pas ordonné l'effacement, il en informe la personnalité en charge du contrôle de la base nationale des données judiciaires prévue à l'article 230-52. »
- Après le mot « sexe » de l'avant dernier alinéa, est inséré l'alinéa suivant : « Le fichier national automatisé des empreintes génétiques est hébergé par la base nationale des données judiciaires. »

Article 14

Le premier alinéa de l'article 706-53-1 du même code est ainsi modifié : « tenue par le service du casier judiciaire » est supprimé et remplacé par « hébergée par la base nationale des données judiciaires ».

Le troisième alinéa de l'article 706-53-10 est complété par la phrase suivante : « Lorsque le procureur de la république n'ordonne pas la rectification ou l'effacement, il en informe la personnalité en charge du contrôle de la base nationale des données judiciaires prévue à l'article 230-52. »

Au premier alinéa de l'article 706-53-11 après le mot « chapitre » est inséré, « ainsi qu'à l'exception de l'interconnexion technique réalisée en application de l'article 230-48. »

Article 15

Le premier alinéa de l'article 706-25-3 du même code est ainsi modifié : « tenue par le service du casier judiciaire national » est supprimé et remplacé par « hébergée par la base nationale des données judiciaires ».

Le quatrième alinéa de l'article 706-25-12 est complété par la phrase suivante : « Lorsque le procureur de la République ou le juge d'instruction n'ordonne pas la rectification ou l'effacement, il en informe la personnalité en charge du contrôle de la base nationale des données judiciaires prévue à l'article 230-52. »

Au premier alinéa de l'article 706-25-13 après le mot « section » est inséré, « ainsi qu'à l'exception de l'interconnexion technique réalisée en application de l'article 230-49. »

Article 16

Au premier alinéa de l'article 777-3 du même code, après le mot « justice » est inséré, « , à l'exception d'une interconnexion technique avec la base nationale des données judiciaires prévue à l'article 230-47, afin d'informer l'autorité gestionnaire du traitement, de la mise à jour d'informations présentes dans le casier judiciaire et dans l'un des traitements hébergés par la base nationale des données judiciaires. »

Article 17

Le troisième alinéa de l'article 706-54 du même code est complété par : « Ce rapprochement n'est opéré qu'avec la catégorie des personnes mises en cause, condamnées ou recherchées, telle que définie à l'article 230-47. En aucun cas ce rapprochement ne peut conduire à l'extraction d'informations relatives aux autres catégories de personnes. »

ANNEXE 3

Projet de décret relatif à la mise en œuvre des traitements à des fins d'exploitation et de rapprochement judiciaires

Publics concernés : personnes mises en cause, victimes et témoins lors de procédures d'enquêtes judiciaires, militaires de la gendarmerie nationale et autres agents de l'Etat investis de pouvoirs d'enquête judiciaire.

Objet : le rapprochement d'informations sur les modes opératoires ainsi que l'exploitation des données recueillies ou générées au cours d'une même enquête par les unités de gendarmerie et les services de police chargés d'une mission de police judiciaire.

Entrée en vigueur : le texte entre en vigueur le lendemain de sa publication.

Notice : le décret encadre la mise en œuvre des traitements de données à caractère personnel permettant le rapprochement judiciaire et l'exploitation des données recueillies ou générées au cours d'une même enquête. Il définit la finalité de ces traitements ainsi que les modalités de collecte, la nature et la durée de conservation de ces données. Il délimite, par ailleurs, les catégories de personnes ayant accès aux données, celles qui peuvent en être légitimement destinataires et les modalités d'habilitation de ces personnes.

Le texte précise, en outre, les modalités de traçabilité des investigations réalisées et de la provenance des informations et données recueillies ou générées.

Article 1

Le décret n°2012-687 du 7 mai 2012 relatif à la mise en œuvre de logiciels de rapprochement judiciaire à des fins d'analyse criminelle est abrogé.

Article 2

Dans les conditions de l'article R. 40-40 du code de procédure pénale tel qu'il résulte du présent texte, le ministre de l'intérieur (direction générale de la police nationale, direction générale de la gendarmerie nationale, préfecture de police et direction générale des douanes) est autorisé à mettre en œuvre les traitements de données à caractère personnel ayant pour finalité l'exploitation des données et le rapprochement d'informations sur les modes opératoires réunies au cours d'une même enquête par les unités de gendarmerie, les services de police et le service national de douane, chargés d'une mission de police judiciaire dans le cadre :

1° Des enquêtes de flagrance ou des enquêtes préliminaires et des investigations exécutées sur commission rogatoire relatives à des crimes et délits punis d'une peine d'emprisonnement ; 2° Des procédures de recherche des causes de la mort ou d'une disparition prévues par les articles 74 et 74-1 du code de procédure pénale.

Article 3

Les données à caractère personnel et informations exploitées au sein des traitements mentionnés à l'article 2 ne peuvent provenir que des données, pièces et documents de procédures judiciaires déjà détenus par les services visés à l'article 2.

Les traitements mis en œuvre peuvent contenir des données à caractère personnel de la nature de celles mentionnées au I de l'article 6 de la loi du 6 janvier 1978 susvisée dans les seuls cas où ces données résultent de la nature ou des circonstances de l'infraction ou se rapportent à des signes physiques particuliers, objectifs et permanents, en tant qu'éléments de signalement des personnes, dès lors que ces éléments sont nécessaires à la mise en œuvre des finalités mentionnées à l'article 230-20 du code de procédure pénale.

Article 4

Ont accès aux données à caractère personnel et aux informations mentionnées à l'article 2 les personnes visées à l'article 230-25 du code de procédure pénale.

Peuvent être destinataires de ces données et informations :

1° Les officiers et agents de police judiciaire de la police nationale, du service national de douane judiciaire, et de la gendarmerie nationale, pour les recherches relatives aux infractions dont ils ont à connaître ;

2° Les organismes de coopération internationale en matière de police judiciaire et les services de police étrangers, dans les conditions prévues à l'article 24 de la loi du 18 mars 2003 susvisée.

Article 5

Les accès à l'infrastructure technique hébergeant les traitements de données mis en œuvre au titre des présentes, font l'objet d'une traçabilité permettant l'identification de l'ensemble des accès horodatés. Ces données sont archivées et placées sous scellés selon les modalités de l'article R40-40 du Code de procédure pénale tel qu'il résulte du présent texte.

Article 6

I. – Conformément à l'article 107 de la loi du 6 janvier 1978, le droit d'information et le droit d'opposition prévus aux susvisée ne s'appliquent pas au présent traitement.

II. - Conformément aux dispositions aux articles 104 et 105 de la même loi, les droits d'accès et de rectification s'exercent auprès de la Commission nationale de l'informatique et des libertés.

Article 7

La mise en œuvre des traitements mentionnés à l'article 2 par le directeur général de la police nationale, le directeur général de la gendarmerie nationale ou le préfet de police s'accompagne de l'envoi à la Commission nationale de l'informatique et des libertés d'un engagement de conformité faisant référence au présent décret accompagné d'un dossier de présentation de l'infrastructure technique utilisée par les agents et militaires habilités.

Cette infrastructure doit notamment permettre d'établir la provenance des données introduites dans un traitement mis en œuvre au titre des présentes, et permettre la traçabilité complète des corrélations entre les résultats obtenus et la provenance des données introduites.

Article 8

L'intitulé du chapitre III du titre IV du livre Ier de la partie réglementaire du Code de procédure pénale, est remplacé par : « Des traitements d'exploitation judiciaire ».

Article 9

L'article R40-40 du même Code de procédure pénale est ainsi modifié :

- Au premier alinéa, les mots « logiciels de rapprochement judiciaire » sont remplacés par « traitements destinés à exploiter les données et à faciliter le rapprochement d'informations »
- Au troisième alinéa, le mot « logiciels » est remplacé par « traitements ».

- Le quatrième alinéa les mots « l'exploitation des enquêtes et investigations » sont remplacés par « les traitements destinés à exploiter les données et à faciliter le rapprochement d'informations ». Le mot « donne » est remplacé par « donnent ». Après le mot « procédure » est inséré : « Des rapports intermédiaires peuvent être établis à tout moment par les agents et militaires habilités, ou à la demande du magistrat ayant autorisé la mise en œuvre du traitement. » A la dernière phrase, avant le mot « une » est inséré : « Lors de l'effacement des données prévu à l'article 230-22, ». Après le mot « exploitées », la fin de la phrase est remplacée par « est placée sous scellés ou scellés numériques. »

Article 10

Au premier alinéa de l'article R40-41 du même Code, les mots « et la mise à jour » sont supprimés et le mot « logiciels » est remplacé par « traitements. »

Article 11

Le présent décret est applicable sur l'ensemble du territoire de la République.

Article 12

Le garde des sceaux, ministre de la justice et des libertés, et le ministre de l'intérieur, de l'outre-mer, des collectivités territoriales et de l'immigration sont chargés, chacun en ce qui le concerne, de l'exécution du présent décret, qui sera publié au Journal officiel de la République française.

ANNEXE 4

Projet de décret pris en application des dispositions relatives à la base nationale des données judiciaires

Article 1

Le titre IV du livre Ier de la partie réglementaire du Code de procédure pénale, est complété par un chapitre IV ainsi rédigé :

Chapitre IV

De la base nationale des données judiciaires

Art. R40-57. – Les traitements automatisés de données à caractère personnel suivants sont hébergés dans la base nationale des données judiciaires :

1° le traitement des antécédents judiciaires prévus aux articles 230-6 et suivants ;

2° le bureau d'ordre national automatisé des procédures judiciaires et du traitement automatisé « Cassiopée » prévu à l'article 48-1 ;

3° le fichier des personnes recherchées prévu à l'article 230-19 ;

4° le fichier automatisé des empreintes digitales prévu par le décret n°87-249 du 8 avril 1987 relatif au fichier automatisé des empreintes digitales géré par le ministère de l'intérieur ;

5° le fichier national automatisé des empreintes génétiques prévu aux article 706-54 et suivants ;

6° le fichier judiciaire national automatisé des auteurs d'infractions sexuelles ou violentes prévu aux articles 706-53-1 et suivants ;

7° le fichier judiciaire national automatisé des auteurs d'infractions terroristes prévu aux articles 706-25-3 et suivants.

Art. R40-58. - En application de l'article 230-51, toutes les données de traçabilité d'utilisation de la base nationale des données judiciaires sont conservées pendant une durée de trois ans. Elles permettent l'identification de la personne ayant procédé à l'utilisation, la date et l'heure, ainsi que l'intégralité des opérations réalisées.

La personne qualifiée et les membres du comité prévus à l'article 230-52 ont un accès complet et permanent aux informations de traçabilité.

Ces informations, préalablement anonymisées, peuvent donner lieu à des exploitations statistiques.

Art. R40-59. – La base nationale des données judiciaires stocke et enregistre les catégories de données à caractère personnel et informations suivantes :

1° l'intégralité des données et informations contenues dans les traitements hébergés en application de l'article R40-57, dans le respect du code unique prévu par l'article 230-47.

2° les données et informations de traçabilité en application de l'article R40-58 :

- identité (nom, prénom, identifiant, le cas échéant numéro de matricule) ;
- service, unité ou structure auquel appartient la personne ;
- adresse IP de connexion ;

- date, heure et durée de la connexion ;
- nature des opérations effectuées.

Art. R40-60. - La base nationale des données judiciaires est placée sous le contrôle d'une personnalité qualifiée, désignée pour une durée de cinq ans non renouvelable par arrêté du garde des sceaux, ministre de la justice, et assistée par un comité composé de cinq membres.

Cette personnalité peut ordonner toutes mesures nécessaires à l'exercice de son contrôle. Cette personnalité et les membres du comité de contrôle disposent d'un accès permanent au service du casier judicaire ainsi qu'en tout lieu permettant de se connecter à la base nationale des données judiciaires.

Cette personnalité est informée de toutes les demandes d'accès ou de rectification relatives aux informations propres à la base nationale des données judiciaires ainsi qu'aux informations contenues dans les traitements automatisés de données à caractère personnel hébergés.

Elle établit un rapport annuel qu'elle adresse au garde des sceaux, ministre de la justice.

Les pouvoirs qui lui sont confiés s'exercent sans préjudice du contrôle exercé par la Commission nationale de l'informatique et des libertés en application des dispositions et selon les modalités prévues par les articles 101,105,107 et 108 de la loi n°78-17 du 6 janvier 1978.

Art. R40-61. - Le comité mentionné à l'article précédent comprend :

a) Un sénateur et un député respectivement choisis par le président du Sénat, après chaque renouvellement partiel du Sénat, et par le président de l'Assemblée nationale, pour la durée de la législature, sur proposition de la commission compétente de chaque assemblée ;

b) Un magistrat du siège honoraire de la Cour de cassation, désigné pour une durée de cinq ans non renouvelable par arrêté du garde des sceaux, ministre de la justice ;

c) Une personnalité qualifiée, désignée pour une durée de cinq ans non renouvelable par arrêté du garde des sceaux, ministre de la justice, sur proposition du ministre chargé des communications électroniques ;

d) Une personnalité qualifiée, désignée pour une durée de cinq ans non renouvelable par arrêté du garde des sceaux, ministre de la justice, sur proposition du ministre de l'intérieur.

Art. R40-62. – Pour la catégorie des personnes prévue au 1° de l'article R40-59, en application de l'article 107 de la loi n°78-17 du 6 janvier 1978, les droits d'information et d'opposition font l'objet d'une restriction et ne s'appliquent pas au présent traitement. Les droits d'accès et de rectification s'exercent de manière indirecte dans les conditions prévues l'article 108 de la loi n°78-17 du 6 janvier 1978.

Pour la catégorie des personnes prévue au 2° de l'article R40-59, les droits d'accès et de rectification s'exercent auprès de la personnalité prévue à l'article 230-52.

Art. R40-63. - Les présentes dispositions entrent en vigueur dans les six mois qui suivent la publication du décret.

Article 2

Au début du premier alinéa de l'article R40-25 du Code de procédure pénale, est inséré « Dans le respect des conditions fixées par l'article 230-47, »

L'article R40-30 est ainsi modifié : « En application des articles R40-58 et R40-59, la nature administrative ou judiciaire de la consultation est enregistrée au sein des opérations effectuées. »

L'article R40-31 est ainsi modifié :

- Au début du premier alinéa est inséré « Sans préjudice des dispositions prévues à l'article 230-52, »
- Un nouvel alinéa est ainsi ajouté : « Le procureur de la République ou le magistrat mentionné à l'article 230-9 informe la personnalité en charge du contrôle de la base nationale des données judiciaires prévue à l'article 230-52 de toute demande de rectification ou d'effacement dont il a été saisi. »

Dans la première phrase du deuxième alinéa de l'article R40-31-1, les mots « l'intéressé peut » sont remplacés par « il en informe la personnalité en charge du contrôle de la base nationale des données judiciaires prévue à l'article 230-51. L'intéressé peut alors, ».

L'article R40-32 est ainsi modifié :

- Au quatrième alinéa, après le mot traitement est ajouté « ainsi qu'à la personnalité en charge du contrôle de la base nationale des données judiciaires prévue à l'article 230-52. »
- Au dernier alinéa, après « 1978 », il est ajouté « ainsi que du contrôle prévu à l'article R40-60, ».

Après le mot « traitement », l'article R40-34 est complété par « , ainsi qu'à la personnalité en charge du contrôle de la base nationale des données judiciaires prévue à l'article 230-52. »

Article 3

L'article R15-33-66-5 du même code est ainsi modifié :

- Au début du premier alinéa est inséré « Sans préjudice des dispositions prévues à l'article 230-51, »
- Au dernier alinéa, après le mot « adresse » est inséré « , ainsi qu'à la personnalité en charge du contrôle de la base nationale des données judiciaires prévue à l'article 230-52, »

L'article R15-33-66-12 est complété par un dernier alinéa : « Une interconnexion technique au sein de la base nationale des données judiciaires est réalisée en application de l'article 230-49. »

L'article R15-33-66-13 est ainsi modifié : « La traçabilité des opérations effectuées sur le traitement est réalisée conformément aux dispositions de l'article R40-58. »

Article 4

A l'article premier du décret n°2010-569 du 28 mai 2010 relatif au fichier des personnes recherchées, après le mot « recherchées » est inséré « , hébergé par la base nationale des données judiciaires ».

A la dernière phrase de l'article 7, après le mot « données » est inséré « , notamment par la personnalité en charge du contrôle de la base nationale des données judiciaires prévue à l'article 230-52 du Code de procédure pénale ».

L'article 8 est ainsi modifié : « La traçabilité des opérations effectuées sur le traitement est réalisée conformément aux dispositions de l'article R40-58 du Code de procédure pénale. »

Article 5

L'article 2 du décret n°87-249 du 8 avril 1987 relatif au fichier automatisé des empreintes digitales géré par le ministère de l'intérieur, est complété par « Il est hébergé par la base nationale des données judiciaires. »

Au dernier alinéa de l'article 7, après le mot « libertés » est inséré « et à la personnalité en charge du contrôle de la base nationale des données judiciaires prévue à l'article 230-52 du Code de procédure pénale ».

Le premier alinéa du II de l'article 7-1 est complété par « Lorsque le procureur de la République estime que leur conservation apparaît nécessaire, il en informe la personnalité en charge du contrôle de la base nationale des données judiciaires prévue à l'article 230-52 du Code de procédure pénale. »

Le sixième alinéa de l'article 7-2 est complété par « Lorsque le procureur de la République conteste la décision, il en informe la personnalité en charge du contrôle de la base nationale des données judiciaires prévue à l'article 230-52 du Code de procédure pénale. »

Après la dernière occurrence du mot « décret » de l'article 9, est inséré « ainsi que pour l'interconnexion technique réalisée en application de l'article 230-49 du Code de procédure pénale. »

Article 6

L'article R53-9 du Code de procédure pénale est ainsi modifié :

- Au premier alinéa, les mots « est mis en œuvre par le service central de la police technique et scientifique du ministère de l'intérieur. » sont remplacés par « conformément à l'article 230-47. »
- Au début du deuxième alinéa est inséré « Sans préjudice des dispositions prévues à l'article 230-52, »

L'article R53-13-5 est complété par « Lorsque le procureur de la République conteste la décision, il en informe la personnalité en charge du contrôle de la base nationale des données judiciaires prévue à l'article 230-52. »

Au début de l'article R53-16 est inséré « Sans préjudice des dispositions prévues à l'article 230-52, »

Au dernier alinéa de l'article R53-17, après la dernière occurrence du mot « libertés » est inséré « et du contrôle exercé par la personnalité en charge du contrôle de la base nationale des données judiciaires prévue à l'article 230-52 ».

Après le dernier mot de l'article R53-19 est inséré, « ainsi qu'à l'exception de l'interconnexion technique réalisée en application de l'article 230-49. »

Article 7

L'article R53-8-23 est complété par un dernier alinéa : « Cette interrogation n'est opérée que sur la catégorie des personnes mises en cause, condamnées ou recherchées, telle que définie à l'article 230-47. En aucun cas cette interrogation ne peut conduire à l'extraction d'informations relatives aux autres catégories de personnes. »

L'article R53-8-31est complété par « Lorsque le procureur de la République conteste la décision, il en informe la personnalité en charge du contrôle de la base nationale des données judiciaires prévue à l'article 230-52. »

L'article R53-8-34 est ainsi modifié :

- Le premier alinéa est remplacé par « Les informations de traçabilité sont conservées selon les conditions prévues à l'article R40-58. »
- Le deuxième alinéa est ainsi modifié : « Ces informations peuvent également être consultées par le magistrat chef du service gestionnaire du fichier et, avec son autorisation, par les personnes qu'il habilite spécialement. »
- Le troisième alinéa est supprimé.

Article 8

L'article R50-51 est complété par un dernier alinéa : « L'interrogation à partir de critères incomplets n'est opérée que sur la catégorie des personnes mises en cause, condamnées ou recherchées, telle que définie à l'article 230-47. En aucun cas cette interrogation ne peut conduire à l'extraction d'informations relatives aux autres catégories de personnes. »

L'article R50-59 est complété par « Lorsque le procureur de la République conteste la décision, il en informe la personnalité en charge du contrôle de la base nationale des données judiciaires prévue à l'article 230-52. »

L'article R50-63 est ainsi modifié :

- Le premier alinéa est remplacé par « Les informations de traçabilité sont conservées selon les conditions prévues à l'article R40-58. »
- Le deuxième alinéa est ainsi modifié : « Ces informations peuvent également être consultées par le magistrat chef du service gestionnaire du fichier et, avec son autorisation, par les personnes qu'il habilite spécialement. »

Le troisième alinéa est supprimé.

Article 9

L'article premier du 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) est complété par un nouvel alinéa : « Une interconnexion technique avec la base nationale des données judiciaires est réalisée en application de l'article 230-49 du Code de procédure pénale. »

Article 10

L'article 4 du décret n°2011-111 du 27 janvier 2011 autorisant la mise en œuvre par le ministère de l'intérieur (direction générale de la gendarmerie nationale) d'un traitement automatisé de données à caractère personnel d'aide à la rédaction des procédures (LRPGN), est ainsi remplacé : « Conformément à l'article 230-49 du Code de procédure pénale, l'application « LRPGN » peut être mise en relation avec la base nationale des données judiciaires prévue à l'article 230-47 pour la mise à jour des données relatives aux procédures judiciaires. »

Article 11

L'article R15-33-66-6 du Code de procédure pénale est ainsi modifié :

- Dans l'énumération du 1° a), avant le mot « identité » est inséré : « - référence procédure » et après « l'étranger ; » est inséré : « - code de nature de l'inscription NATINS ; »
- Dans l'énumération du 1° c), après « dossier ; » est inséré : « , code de nature de l'inscription NATINS »
- Au 2°, après « peine prononcée » est inséré : « et détail de la condamnation ».

Article 12

L'article R40-25 du même code est ainsi modifié :

- Les énumérations des a) et b) du 1°, des a) et b) du 2° et du 3° du quatrième alinéa sont complétées par : « - référence procédure ; »
- Les énumérations du 1° a), du 2° a) et du 3° du quatrième alinéa sont complétées par : « - code de nature de l'inscription NATINS ; »
- Dans les énumérations du 1° a), du 2° a) et du 3° du quatrième alinéa, après « - date et lieu de naissance ; » est inséré « - le cas échéant, date de décès ; » et après « - nationalité ; » est inséré « - langue, dialecte parlé ; ».

Article 13

L'article 3 du décret n°2010-569 du 28 mai 2010 relatif au fichier des personnes recherchées est ainsi modifié :

- Au 1°, après le mot « nationalité », est inséré « , les adresses, les adresses électroniques, les numéros de téléphones, la référence de la procédure, le code de nature de l'inscription NATINS »
- Après le 1° est inséré un 1° bis ainsi rédigé « La langue ou le dialecte parlé ; »
- La première phrase du deuxième alinéa est supprimée et au 2°bis, après photographies est inséré « , notamment les clichés permettant la reconnaissance faciale. »
- Au 3°, les mots « Les motifs » sont remplacés par « La description des faits à l'origine ».

Article 14

Le premier alinéa de l'article 4 du décret n°87-249 du 8 avril 1987 relatif au fichier automatisé des empreintes digitales géré par le ministère de l'intérieur est ainsi modifié :

- Au 1°, après le mot « prénoms » est inséré « surnoms, nationalité, adresses, les adresses électroniques, les numéros de téléphones, langue ou dialecte parlé, ».
- Le 4° est ainsi modifié « La nature de l'affaire, la référence de la procédure et le code de nature de l'inscription NATINS ; »
- Au 5°, après le mot « anthropométriques » est inséré « ou de reconnaissances faciales et le signalement de la personne ».

Le deuxième alinéa de l'article 4 est ainsi modifié :

- Le mot « Les » est remplacé par « En application de l'article R40-59, les »
- Les mots « sont accompagnées des » sont remplacés par « comportent notamment les ».

Le 2° de l'article 7-1 est supprimé.

Article 15

L'article R53-11 du Code de procédure pénale est ainsi modifié :

- Au I. 1°, après le mot « demandé » est inséré « et le code de nature de l'inscription NATINS »
- Le 2° du I. est remplacé par : « les informations de traçabilité prévues à l'article R40-59 ; ».
- Au 3° du I. après « R.53-10 », la fin de phrase est ainsi rétablie : « , la date et le détail de la condamnation. »
- Le 5° du I. est remplacé par « la description des faits ou de l'infraction à l'origine de l'inscription. »
- Au deuxième alinéa du II. après le mot « prénoms, », est inséré « surnoms, sexe, nationalité, adresses, les adresses électroniques, les numéros de téléphones, langue ou dialecte parlé, signalement, les photos permettant la reconnaissance faciale »
- Au deuxième alinéa du II. après le mot « filiation », est inséré « , le cas échéant la date du décès ».

Article 16

L'article R53-8-7 du même code est ainsi modifié :

- Au 1°, après la deuxième occurrence du mot « personne, » est inséré « les adresses électroniques, les numéros de téléphones, la langue ou le dialecte parlé, le signalement, les photos permettant la reconnaissance faciale »
- Au 1°, après la première occurrence du mot « échéant, » est inséré « la date de décès, »

- Au 2°, « - juridiction ayant prononcé la décision ; » est remplacé par « la date et le détail de la condamnation. » et « -date d'exécution ou de fin d'exécution de la peine ou de la mesure ; » est supprimé
- Au 2°, avant « - peines principales ou complémentaires ou mesures prononcées ; » est inséré « « référence procédure et code de nature de l'inscription NATINS ».

L'article R53-8-35 est ainsi modifié :

- Le c) est supprimé ;
- Il est ajouté un nouvel alinéa ainsi rédigé : « Le décès de la personne est sans effet sur les délais prévus dans le présent article. »

Article 17

L'article R50-36 du même code est ainsi modifié :

- Au 1° a), après le mot « nationalités, » est inséré « le signalement, les photos permettant la reconnaissance faciale, les adresses électroniques, les numéros de téléphones, la langue ou le dialecte parlé, »
- Au 1° a), après le mot « échéant » est inséré « la date de décès, ».
- Au 2°, le a) est ainsi modifié « a) Nature, date, numéro de procédure de la décision et code de nature de l'inscription NATINS ; »
- Au 2°, le b) est ainsi remplacé : « la date et le détail de la condamnation ; ».

L'article Article R50-64 est ainsi modifié :

- Le c) est supprimé ;
- Il est ajouté au début du dernier alinéa : « Le décès de la personne est sans effet sur les délais prévus dans le présent article. »

ANNEXE 5

Cartographie issue des dispositions actuelles des traitements appelés à être hébergés par la BNDJ

		Cassiopée	Traitement d'antécédents judiciaires	Fichier des personnes recherchées	Fichier automatisé des empreintes digitales	Fichier national automatisé des empreintes génétiques	Fichier judicaire national automatisé des auteurs d'infractions sexuelles ou violentes	Fichier judicaire national automatisé des auteurs d'infractions terroristes
I	A	Nom	Nom	Nom	Nom	Nom	Nom	Nom
		Nom marital	Nom marital	Nom marital	Nom marital	Nom marital	Nom marital	Nom marital
		Nom d'emprunt officiel	Nom d'emprunt officiel	Nom d'emprunt officiel	Nom d'emprunt officiel	Nom d'emprunt officiel	Nom d'emprunt officiel	Nom d'emprunt officiel
		Prénoms	Prénoms	Prénoms	Prénoms	Prénoms	Prénoms	Prénoms
		Sexe	Sexe	Sexe	Sexe		Sexe	Sexe
		Surnom	Surnom	Surnom			Surnom	Surnom
		Date de naissance	Date de naissance	Date de naissance	Date de naissance	Date de naissance	Date de naissance	Date de naissance
		Age selon expertise						
		Date de décès						
		Lieu de naissance	Lieu de naissance	Lieu de naissance	Lieu de naissance	Lieu de naissance	Lieu de naissance	Lieu de naissance
		Situation familiale	Situation familiale					
		Nbr frères et sœurs						
		Rang dans fratrie						
		Filiation	Filiation	Filiation	Filiation	Filiation	Filiation	Filiation
		Nationalité	Nationalité	Nationalité			Nationalité	Nationalité
		Pièce ident : numéro						
		Pièce ident : date déliv						
		Pièce ident. : aut déliv						
		P. ident : si étrang.						
		Langue, dialecte parlé						
		Adresses	Adresses					
							Adresses (historique)	Adresses (historique)
		Adresses électroniques	Adresses électroniques					
		Téléphones	Téléphones					
		Niveau d'étude						
		Diplômes						
		Distinctions						
		Profession	Profession					
		Code cat. socio-prof.						
		Code nature activité						
		Situation emploi						
		Rais soc employeur						

		Cassiopée	Traitement d'antécédents judiciaires	Fichier des personnes recherchées	Fichier automatisé des empreintes digitales	Fichier national automatisé des empreintes génétiques	Fichier judicaire national automatisé des auteurs d'infractions sexuelles ou violentes	Fichier judicaire national automatisé des auteurs d'infractions terroristes
		Téléphone au travail						
		Fonction élective						
		Immunité						
		Militaires: inf. spécif.						
		Etablissement scolaire						
		Année scolaire : classe						
		Ex. de l'aut. parent.						
		Données bancaires						
	B	Raison sociale	Raison sociale					
		Enseigne commerciale	Enseigne commerciale					
		Sigle	Sigle					
		Forme juridique	Forme juridique					
		Siège social	Siège social					
		SIREN	SIREN					
		SIRET	SIRET					
			Secteur activité					
		Date cess. paiement						
II			Etat de la personne					
			Signalement	Signalement				
			Photo. reconnais. fac.					
					Photo anthropométriq.			
			Photographies autres	Photographies autres				
		Ant. judi. société						
		Condam. passées						
		Actuellement en fugue						

		Cassiopée	Traitement d'antécédents judiciaires	Fichier des personnes recherchées	Fichier automatisé des empreintes digitales	Fichier national automatisé des empreintes génétiques	Fichier judicaire national automatisé des auteurs d'infractions sexuelles ou violentes	Fichier judicaire national automatisé des auteurs d'infractions terroristes
III		Faits - description	Faits - description		Faits - description			
		Récidive						
			Objets de l'enquête					
							Nature de l'infraction	Nature de l'infraction
		Code nat inf. NATINF						
				Motifs de la recherche				
				Actes admin. ou judi.			Actes admin. ou judi.	Actes admin. ou judi.
						Nature de l'affaire		
		Lieux infraction	Lieux infraction				Lieux infraction	Lieux infraction
		Date infraction	Date infraction				Date infraction	Date infraction
			Mode opératoire					
			Photos objets					
			Description objets					
IV	A				Référence procédure	Référence procédure		
		Sit judi dans procédure						
	B	Situation pénale					Situation pénale	Situation pénale
		Sit pén : num écrou						
		Sit pén : date lib. prév.					Sit pén : date lib. prév.	Sit pén : date lib. prév.
		Mode comparution						
		Nature jugement					Nat jug. + date jug.	Nat jug. + date jug.
							Juridiction : décision	Juridiction : décision
		Dom. int./provision						
		Peine prononcée					Peine prononcée	Peine prononcée
						Date condamnation		
							Fin (peine/mesure/exe)	
		Libellé peine						
		Mesure						
		Motifs						
		Obligations					Obligations	Obligations
						Date condam déf		

		Cassiopée	Traitement d'antécédents judiciaires	Fichier des personnes recherchées	Fichier automatisé des empreintes digitales	Fichier national automatisé des empreintes génétiques	Fichier judicaire national automatisé des auteurs d'infractions sexuelles ou violentes	Fichier judicaire national automatisé des auteurs d'infractions terroristes
V				Conduite à tenir				
					Emp. /traces d'emp.			
						Traces/échantillons		
						Info sur échantillons		
						Nom réalisation anal.		
						Si pers disp : lien par.		
							Date notif oblig	Date notif oblig
							Date justif adresse	Date justif adresse
							Périod. oblig présentat.	Périod. oblig présentat.
							Incription pers. Rech.	Incription pers. rech.
							Autres décisions	Autres décisions
								Dép. transfrontaliers
VI	A	Avocat : nom						
		Avocat : nom d'usage						
		Avocat : prénom						
		Avocat : numéro prof.						
		Avocat : barr. rattach.						
		Avocat : adresse cab.						
		Avocat : numé. toque						
		Avocat : adresse élect						
		Avocat : téléphone						
		Avocat : télécopie						
		Avocat : numé. toque						
		Avocat : numé. toque						
	B	Agent FPE : nom						
		Agent FPE : nom usage						
		Agent FPE : prénom						
		Agent FPE : corps/grad						
		Agent FPE : code						
		Agent FPE : fonction						
		Agent FPE : acro serv.						

		Cassiopée	Traitement d'antécédents judiciaires	Fichier des personnes recherchées	Fichier automatisé des empreintes digitales	Fichier national automatisé des empreintes génétiques	Fichier judicaire national automatisé des auteurs d'infractions sexuelles ou violentes	Fichier judicaire national automatisé des auteurs d'infractions terroristes
		Agent FPE : libel serv.						
					Service ayant signalé	Service ayant signalé		
						OPJ : demand enr.		
					Date signalement	Date signalement		
					Lieu d'étab. signalem.			
							Carac exprès enregist.	

Légende des catégories

I	Données identification :
A	des personnes physiques
B	des personnes morales
II	Eléments judiciaires pour les antécédents
III	Les éléments factuels de la procédure
IV	Le suivi judiciaire de la procédure :
A	éléments généraux
B	informations détaillées
V	Données spécifiques aux traitements particuliers
VI	Informations relatives aux intervenants dans la procédure :
A	les avocats
B	les agents (policiers, fonctionnaires du ministère de la justice, etc) et les militaires

ANNEXE 6

Projet d'amélioration de la cartographie des traitements appelés à être hébergés par la BNDJ

		Cassiopée	Traitement d'antécédents judiciaires	Fichier des personnes recherchées	Fichier automatisé des empreintes digitales	Fichier national automatisé des empreintes génétiques	Fichier judicaire national automatisé des auteurs d'infractions sexuelles ou violentes	Fichier judicaire national automatisé des auteurs d'infractions terroristes
I		Nom	Nom	Nom	Nom	Nom	Nom	Nom
		Nom marital	Nom marital	Nom marital	Nom marital	Nom marital	Nom marital	Nom marital
		Nom d'emprunt officiel	Nom d'emprunt officiel	Nom d'emprunt officiel	Nom d'emprunt officiel	Nom d'emprunt officiel	Nom d'emprunt officiel	Nom d'emprunt officiel
		Prénoms	Prénoms	Prénoms	Prénoms	Prénoms	Prénoms	Prénoms
		Sexe	Sexe	Sexe	Sexe	Sexe	Sexe	Sexe
		Surnom	Surnom	Surnom	Surnom	Surnom	Surnom	Surnom
		Date de naissance	Date de naissance	Date de naissance	Date de naissance	Date de naissance	Date de naissance	Date de naissance
		Age selon expertise						
		Date de décès	Date de décès		Date de décès	Date de décès	Date de décès	Date de décès
		Lieu de naissance	Lieu de naissance	Lieu de naissance	Lieu de naissance	Lieu de naissance	Lieu de naissance	Lieu de naissance
		Situation familiale	Situation familiale					
		Nbr frères et sœurs						
		Rang dans fratrie						
		Filiation	Filiation	Filiation	Filiation	Filiation	Filiation	Filiation
		Nationalité	Nationalité	Nationalité	Nationalité	Nationalité	Nationalité	Nationalité
		Pièce ident : numéro						
		Pièce ident : date déliv						
		Pièce ident. : aut déliv						
		P. ident : si étrang.						
	A	Langue, dialecte parlé	Langue, dialecte parlé	Langue, dialecte parlé	Langue, dialecte parlé	Langue, dialecte parlé	Langue, dialecte parlé	Langue, dialecte parlé
		Adresses	Adresses	Adresses	Adresses	Adresses	Adresses	Adresses
		Adresses électroniques	Adresses électroniques	Adresses électroniques	Adresses électroniques	Adresses électroniques	Adresses électroniques	Adresses électroniques
		Téléphones	Téléphones	Téléphones	Téléphones	Téléphones	Téléphones	Téléphones
		Niveau d'étude						
		Diplômes						
		Distinctions						
		Profession	Profession					
		Code cat. socio-prof.						
		Code nature activité						
		Situation emploi						
		Rais soc employeur						
		Téléphone au travail						

		Cassiopée	Traitement d'antécédents judiciaires	Fichier des personnes recherchées	Fichier automatisé des empreintes digitales	Fichier national automatisé des empreintes génétiques	Fichier judicaire national automatisé des auteurs d'infractions sexuelles ou violentes	Fichier judicaire national automatisé des auteurs d'infractions terroristes
		Fonction élective						
		Immunité						
		Militaires: inf. spécif.						
		Etablissement scolaire						
		Année scolaire : classe						
		Ex. de l'aut. parent.						
		Données bancaires						
		Raison sociale	Raison sociale					
		Enseigne commerciale	Enseigne commerciale					
		Sigle	Sigle					
		Forme juridique	Forme juridique					
	B	Siège social	Siège social					
		SIREN	SIREN					
		SIRET	SIRET					
			Secteur activité					
		Date cess. paiement						
			Etat de la personne					
			Signalement	Signalement	Signalement	Signalement	Signalement	Signalement
			Photo. reco. fac./anthro.		Photo. reco. fac./anthro	Photo. reco. fac./anthro	Photo. reco. fac./anthro	Photo. reco. fac./anthro.
	II		Photographies autres	Photographies autres				
		Ant. judi. société						
		Condam. passées						
		Actuellement en fugue						

		Cassiopée	Traitement d'antécédents judiciaires	Fichier des personnes recherchées	Fichier automatisé des empreintes digitales	Fichier national automatisé des empreintes génétiques	Fichier judicaire national automatisé des auteurs d'infractions sexuelles ou violentes	Fichier judicaire national automatisé des auteurs d'infractions terroristes
III		Faits - Desc. infraction	Faits - Desc. Infraction	Faits - Desc. Infraction	Faits - Desc. Infraction	Faits - Desc. Infraction	Faits - Desc. Infraction	Faits - Desc. Infraction
		Code nat inf. NATINF						
		Récidive						
				Actes admin. ou judi.			Actes admin. ou judi.	Actes admin. ou judi.
		Lieux infraction	Lieux infraction				Lieux infraction	Lieux infraction
		Date infraction	Date infraction				Date infraction	Date infraction
			Mode opératoire					
			Photos objets					
			Description objets					
IV	A	Référence procédure	Référence procédure	Référence procédure	Référence procédure	Référence procédure	Référence procédure	Référence procédure
		Sit judi dans procédure						
		Code NATINS	Code NATINS	Code NATINS	Code NATINS	Code NATINS	Code NATINS	Code NATINS
	B	Situation pénale					Situation pénale	Situation pénale
		Sit pén : num écrou						
		Sit pén : date lib. prév.					Sit pén : date lib. prév.	Sit pén : date lib. prév.
		Mode comparution						
		Date et histo condam.				Date et histo condam.	Date et histo condam.	Date et histo condam.
		Peine prononcée					Peine prononcée	Peine prononcée
		Libellé peine						
		Mesure						
		Motifs						
		Obligations					Obligations	Obligations
		Dom. int./provision						

		Cassiopée	Traitement d'antécédents judiciaires	Fichier des personnes recherchées	Fichier automatisé des empreintes digitales	Fichier national automatisé des empreintes génétiques	Fichier judicaire national automatisé des auteurs d'infractions sexuelles ou violentes	Fichier judicaire national automatisé des auteurs d'infractions terroristes
V				Conduite à tenir				
					Emp. /traces d'emp.			
						Traces/échantillons		
						Info sur échantillons		
						Nom réalisation anal.		
						Si pers disp : lien par.		
							Date notif oblig	Date notif oblig
							Date justif adresse	Date justif adresse
							Périod. oblig présentat.	Périod. oblig présentat.
							Incription pers. Rech.	Incription pers. rech.
							Autres décisions	Autres décisions
								Dép. transfrontaliers
VI	A	Avocat : nom						
		Avocat : nom d'usage						
		Avocat : prénom						
		Avocat : numéro prof.						
		Avocat : barr. rattach.						
		Avocat : adresse cab.						
		Avocat : numé. toque						
		Avocat : adresse élect						
		Avocat : téléphone						
		Avocat : télécopie						
		Avocat : numé. toque						
		Avocat : numé. toque						
	B	Opérateur : nom	Opérateur : nom	Opérateur : nom	Opérateur : nom	Opérateur : nom	Opérateur : nom	Opérateur : nom
		Opérateur : nom usage	Opérateur : nom usage	Opérateur : nom usage	Opérateur : nom usage	Opérateur : nom usage	Opérateur : nom usage	Opérateur : nom usage
		Opérateur : prénom	Opérateur : prénom	Opérateur : prénom	Opérateur : prénom	Opérateur : prénom	Opérateur : prénom	Opérateur : prénom
		Opérateur : corps/grad	Opérateur : corps/grad	Opérateur : corps/grad	Opérateur : corps/grad	Opérateur : corps/grad	Opérateur : corps/grad	Opérateur : corps/grad
		Opérateur : code	Opérateur : code	Opérateur : code	Opérateur : code	Opérateur : code	Opérateur : code	Opérateur : code
		Opérateur : fonction	Opérateur : fonction	Opérateur : fonction	Opérateur : fonction	Opérateur : fonction	Opérateur : fonction	Opérateur : fonction
		Opérateur : acro serv.	Opérateur : acro serv.	Opérateur : acro serv.	Opérateur : acro serv.	Opérateur : acro serv.	Opérateur : acro serv.	Opérateur : acro serv.

		Cassiopée	Traitement d'antécédents judiciaires	Fichier des personnes recherchées	Fichier automatisé des empreintes digitales	Fichier national automatisé des empreintes génétiques	Fichier judicaire national automatisé des auteurs d'infractions sexuelles ou violentes	Fichier judicaire national automatisé des auteurs d'infractions terroristes
		Opérateur : libel. serv.	Opérateur : libel. serv.	Opérateur : libel. serv.	Opérateur : libel. serv.	Opérateur : libel. serv.	Opérateur : libel. serv.	Opérateur : libel. serv.
		Date opération	Date opération	Date opération	Date opération	Date opération	Date opération	Date opération
		Lieu opération	Lieu opération	Lieu opération	Lieu opération	Lieu opération	Lieu opération	Lieu opération
							Carac exprès enregist.	

Légende des catégories

I	Données identification :
A	des personnes physiques
B	des personnes morales
II	Eléments judiciaires pour les antécédents
III	Les éléments factuels de la procédure
IV	Le suivi judiciaire de la procédure :
A	éléments généraux
B	informations détaillées
V	Données spécifiques aux traitements particuliers
VI	Informations relatives aux intervenants dans la procédure :
A	les avocats
B	les agents (policiers, fonctionnaires du ministère de la justice, etc) et les militaires

BIBLIOGRAPHIE

I – Bibliographie générale

01NET, *Un traqueur d'activité balance un meurtrier*, 01net n°918, 20 octobre 2019.

ALAMAR Bruno, *Pour la libre circulation des données*, Le monde Eco et Entreprise, 11 avril 2018.

Aujourd'hui en France, 5 novembre 2017, *Terrorisme Adapter « nos règles » au « risque durable »*, p. 5

BOULEZ Jacques, *Expertises judiciaires – Désignation et mission de l'expert – Procédure selon la juridiction,* DELMAS, 13ème édition.

CARDON Dominique, *Réseaux sociaux de l'Internet,* Communications 2011/1 n°88, p.141-148.

CASILLI Antonio, *En attendant les robots – enquête sur le travail du clic,* SEUIL, 2019.

DEFOSSEZ Adrien, *Soutien social et réseau personnel au cœur de l'expérience du cancer,* thèse soutenue le 9 décembre 2014.

DENOUËL Julie et GRANJON Fabien, *Communiquer à l'ère numérique,* Edition Mines ParisTech, 2011.

DUPRAT Florent, *Trente gendarmes formés pour enquêter sur le numérique,* La dépêche du Midi, 27 novembre 2018.

GROSSETTI Michel, *Que font les réseaux sociaux aux réseaux sociaux ? Réseaux personnels et nouveaux moyens de communication,* Réseaux n°184-185, 2014/2-3 p. 187.

HAS, *procédure de certification V2014 des établissements de santé*.

LECHENET Alexandre, *Sans les nouvelles technologies, ces enquêtes journalistiques n'auraient probablement pas abouti*, Ecrans, 13 oct. 2013.

Le Monde, 8 septembre 2008, p. 10, *Fichier Edvige : les points inquiétants pour les libertés.*

Le Monde Spécial, 2 novembre 2017, *Un an, 11 mois et 18 jours d'urgence*, p. 2.

Le Monde, 23 mars 2018, *Attaques de Carcassonne et Trèbes : ce que l'on sait.*

Libération, 4 septembre 2008, n°8501, *La vigilance autour d'Edvige.*

Libération, 12 septembre 2013, *La mémoire longue conservation de la justice*.

L'Est Républicain, *Un officier de police suspendu*, Lorraine, mardi 26 février 2019, p.6

L'Usine Digitale, 22 novembre 2017, *Uber a caché le vol de données de 50 millions de clients et 7 millions de chauffeurs*.

Le Parisien, 1er décembre 2017, *Le mystère des bébés de Galfingue élucidé 14 ans après*.

MEDDAH Hassan, *Cyber cherche experts désespérément,* L'usine Nouvelle n°3642, 16 janvier 2020.

MICHEL Jean-Charles, *Les disques durs ne résistent pas à l'enquêteur*, Ouest France Morbihan, 12 mars 2012.

Ouest-France Vendée, 5 mai 2012, *Départ du procureur de la République vers Nantes.*

ORTIZ Sébastien, *Les commissariats rapprochés 2 par 2*, L'Eclaireur du Gâtinais,1 janv. 2020.

Revue Lamy Droit de l'immatériel, 1er août 2017, *Interrogations sur la portée territoriale du droit au déréférencement,* n°140.

RUELLAN François et MARIE Nathalie, *Droit et pratique de l'expertise judiciaire civile,* LexisNexis.

VILLANI Cédric, *rapport de synthèse France intelligence artificielle,* 28 mars 2018.

II – Bibliographie informatique et systèmes d'information

O1NET, *Sécurisez l'accès à votre compte UBUNTU*, 01net, 6 février 2019.

01NET, *Les juges remettent en cause la géolocalisation*, 01NET, 2 oct. 2019.

ANSSI, *Recommandations de sécurité relatives* à TLS, 2016.

BOERO Alexandre, *Kaspersky a recensé 105 millions d'attaques contre des objets connectés au premier semestre*, Clubic, 17 oct. 2019.

BOUCQ Isabelle, *Profession administrateur réseau*, Micro Hebdo, 2 mars 2005.

BOURHA Nadia, *SaaS, PaaS, IaaS... que choisir?* Direction informatique, 28 octobre 2013.

CALVAR Patrick (directeur général de la sécurité intérieure), *audition du 10 mai 2016 devant Commission de la défense nationale et des forces armées de l'Assemblée Nationale*, Compte rendu n° 47.

COHEN Jo, *Données personnelles,* PUBLINET Sécurité Informatique, n°418, 3 juin 2014.

DAUERER Norman J. and KEKKEY Edward E., *Front end for file access controller*, Nov. 21, 1995.

DELATTRE Laurent, *La gouvernance des données au coeur des audits en 2020*, ITforBusiness, 15 novembre 2019

DENIS Jérôme, *L'informatique et sa sécurité - Le souci de la fragilité technique*, Réseaux 2012/1 (n° 171), pages 161 à 187.

DURAND André, *Gestion des identités et des accès : les grandes tendances de 2020*, Silicon, 6 janvier 2020.

DUTHEIL Christophe, *L'usine du futur s'édifie brique par brique,* ElectroniqueS n°64, 1er octobre 2015.

INDUSTRIE ET TECHNOLOGIES, *A Elancourt, Thales scrute 3 milliards d'événements de sécurité par jour*, Industrie et Technologies, 11 mars 2016.

MJOLNES Stig and OLIMID Ruxandra, *Easy 4G/LTE IMSI Catchers for Non-Programmers*, Cornell University, 15 feb. 2017.

GENGEMBRE Charles, *Information sensible d'entreprise : une attention de tous les instants*, ItforBusiness, 14 mars 2018.

INTEROP-Vlab, *Secured exchanges of data along the logistic chains,* 7 octobre 2015.

KAPFER Philippe, *Internal Hacking et contre-mesures en environnement Windows,* Editions ENI.

KAMBATLA, KARTHIK and KOLLIAS, GIORGOS and KUMAR, VIPIN and GRAMA, ANANTH, *Trends in big data analytics*, Journal of Parallel and Distributed Computing, pages 2561-2573, 2014, Elsevier.

LANDRY Pierre, *À la recherche de l'architecture de stockage absolue*, ITforBusiness, 1er octobre 2014.

LEMAIRE Thierry, *Gemplus veut sécuriser les extranets d'entreprise avec Gemsafe Enterprise*, Sécurité Informatique, 1 juin 2001.

LEMOINE Vincent, *Le régime juridique des constatations policières sur internet,* L'Harmattan.

LUSSAN Pierre-Louis, *Respect de la protection de la vie privée : bien plus qu'une simple case à cocher pour les entreprises,* Silicon, 12 dec. 2019.

Norme ISO 27001, *Techniques de sécurité – Systèmes de gestion de la sécurité de l'information*, Afnor.

Norme ISO 27002, *Techniques de sécurité – Code de bonne pratique pour la gestion de la sécurité de l'information*, Afnor.

Observatoire des libertés et du numérique, *Chiffrement, sécurité et libertés, positionnement de l'Observatoire*, janvier 2017.

PARISOT Thierry, *L'organisation mise en place aux achats sert de modèle à la DSI*, ITforBusiness, 1er mars 2015, entretien avec Charles-Henri VOLLET, Directeur des achats et des systèmes d'information groupe, Mersen.

POUPARD Guillaume (Directeur général de l'ANSSI), *lettre du 24 mars 2016 adressée aux ministères de la Défense, de l'Économie, de l'Intérieur et de la Justice.*

REZAEI Reza, CHIEW Thiam-kian, LEE Sai-peck, *A review of interoperability assessment models,* Journal of Zhejiang University-SCIENCE C, www.springerlink.com, 2013.

SAVART Michel (Directeur du laboratoire de police scientifique de Lyon), *l'expertise scientifique en matière pénale,* Dalloz AJ pénal 2006 p72.

Silicon, *Gestion des identités et des accès : comment choisir entre les solutions logicielles et le Saas*, Silicon site web, 1 avril 2019.

Sécurité informatique, *Evidian classe les méthodes d'authentification les plus utilisées*, Sécurité informatique n°352, 24 mai 2011.

TOTEL Jérôme, *Multicloud : les questions à se poser avant de définir sa stratégie,* Silicon, 28 mars 2019.

VARANDAT Marie, *Actia optimise ses process à l'échelle internationale avec un PLM*, ITforBusiness, 16 mars 2018.

WALLIANALLUR RAGHUPATHI and VIJU RAGHUPATHI*, Big data analytics in healthcare : promise and potential,* Health Information science and systems, 2014.

III – Bibliographie juridique

A. Manuels, traités, ouvrages

AMBROISE-CASTEROT Coralie et BONFILS Philippe, *Procédure pénale,* puf Thémis droit, 2011.

BOULEZ Jacques, *Expertises judiciaires – Désignation et mission de l'expert – Procédure selon la juridiction*, 13ème édition, DELMAS.

BOULOC Bernard, *Procédure pénale*, 24ème édition, Dalloz.

CADIET Loïc et JEULAND Emmanuel, *Droit judiciaire privé,* LexisNexis.

CASTALDO André et MAUSIN Yves, *Introduction historique au droit,* 4ème édition, Dalloz.

CONTE Philippe et LARGUIER Jean, Procédure pénale, 24ème édition, Dalloz.

CORNU Gérard, *Vocabulaire juridique*, 10ème édition, puf.

De FROUVILLE Olivier, *La preuve pénale, Internationalisation et nouvelles technologies,* La documentation Française.

DESPORTES Frédéric et LAZERGES-COUSQUER Laurence, *Traité de procédure pénale,* Economica.

DEVAUX Olivier, *Histoire des institutions de la France (1er – XIVème siècle)*, L'Hermès.

DREYER Emmanuel MOUYSSET Olivier, *Procédure pénale,* LGDJ, 2019.

GUINCHARD Serge et BUISSON Jacques, *Manuel de Procédure pénale,* LexisNexis, 10ième édition.

LEROY Jacques, *Procédure pénale,* 4ème édition, LGDJ.

MERLE Roger et VITU André, *Traité de droit criminel – Problèmes généraux de la science criminelle, Droit pénal général,* Editions CUJAS, 7ème édition.

MERLE Roger et VITU André, *Traité de droit criminel – Procédure pénale,* Editions CUJAS, 5ème édition.

MORVAN Patrick, *Criminologie*, LexisNexis, 3ème édition.

PORCHY-SIMON Stéphanie, *Droit Civil – Les obligations,* Dalloz, 9ème édition.

POUYANNE Julia, *L'auteur moral de l'infraction*, Presses universitaires d'Aix-Marseille, 2003.

PRADEL Jean, *Procédure pénale*, 18ème édition Collection Référence, Edition Cujas.

PRADEL Jean et VARINARD André, *Les grands arrêts de la procédure pénale,* 8ème édition, Dalloz.

RASSAT Marie-Laure*, Procédure pénale,* 2ème édition, Ellipses.

ROBERT Jacques-Henri, *Droit pénal général*, 5ème édition, Puf Droit.

ROUSSEL Gildas, *Procédure pénale*, 8ème édition, Vuibert.

VERGES Etienne, *Procédure pénale,* 4ème édition, LexisNexis.

VERNY Edouard, *Procédure pénale*, Dalloz, 6ème édition,

B. Articles, notes, études et chroniques

ALLAIN Emmanuelle, *Fichiers d'antécédents : un rapport préoccupant*, Dalloz AJ pénal 2013.

AMBROISE-CASTEROT Coralie et COMBEAU Chantal, *La procédure pénale dans la balance : entre secret et transparence*, Dalloz, Les cahiers de la justice 2014 p. 373.

AMBROISE-CASTEROT Coralie, *Validation européenne des écoutes téléphoniques incidentes d'avocat,* Dalloz, AJ pénal 2016 p. 427.

BAUER Alain et SOULLEZ Christophe, *Les fichiers de police et de gendarmerie,* puf collection Que sais-je ?

BEAUVALLET Olivier, *Entraide judiciaire internationale – Dispositions générales*, JurisClasseur Procédure pénale Fasc. 20, 2018.

BEGRANGER Gérald, *Le contrôle des fichiers de police par les juges*, Dalloz, AJ pénal 2014.

BERGE Jean-Sylvestre et LE METAYER Daniel, *Données - Phénomènes de masse et droit des données,* LexisNexis, Communication commerce électronique, décembre 2018.

BERGERE Anne-Laure, *Le juge des libertés et de la détention, entre indépendance statutaire et dépendances matérielles*, Dalloz AJ Pénal 2019 p.120.

BIANCHI Virginie, *L'effacement des fichiers ou le nouveau mythe de Sisyphe*, Dalloz, AJ Pénal 2007.

BONIS Evelyne, *Magistrature – L'indépendance des magistrats du parquet ou le difficile exercice d'équilibriste du Conseil constitutionnel,* JurisClasseur, Droit pénal n°2, étude 3, février 2018.

BONIS Evelyne et PELTIER Virginie, *Droit de la peine*, 3ème édition, LexisNexis.

BOULAKRAS Haffide, *La procédure pénale numérique (PPN) : promesses, apports et réalisations*, LexisNexis, Droit pénal n°3, mars 2020.

BOURCIER Danièle et DE FILIPPI Primavera, *L'Open Data : universalité du principe et diversité des expériences* ?, Semaine Juridique Administrations et Collectivités territoriales, n° 38, Septembre 2013.

BRUNAUX Geoffray, *Cloud computing, protection des données : et si la solution résidait dans le droit des contrats spéciaux ?*, Recueil Dalloz, 2013.

BUISSON Jacques, *Crimes et délits flagrants,* JurisClasseur Procédure pénale Fasc. 20.

BUISSON Jacques, *Preuve*, Répertoire de droit pénal et de procédure pénale, Dalloz.

CABON Sarah-Marie, *Atteintes aux systèmes de traitement automatisé de données – L'influence du cyber espace sur la criminalité économique et financière,* LexisNexis, Droit pénal n°3, mars 2018, étude 5.

CAMOUS Eric, *Les procédures incidentes : le point de vue d'un magistrat du parquet,* Gazette du Palais, 19 juillet 2016, n°271a5.

CAPDEPON Yannick, *Ecoutes judiciaires – La nullité d'une écoute téléphonique sur la ligne d'un tiers,* LexisNexis, Droit pénal n°12, décembre 2017.

CASTETS-RENARD Céline, *Réforme de la LIL et transposition de la directive à des fins de coopération policière et judiciaire pénale*, Dalloz IP/IT 2018 p.480.

CHAVENT-LECLÈRE Anne-Sophie, *Affaiblissement de la distinction entre réquisition afin d'obtenir des documents et réquisition afin d'obtenir des informations,* LexisNexis, Procédures n° 2, Février 2014, comm. 56.

CHEVALLIER Frédéric et BAILLARD Denys, *Le numérique au service du contradictoire,* LexisNexis, Droit pénal n°3, mars 2018, entretien 3.

CHOPIN Frédérique, *Modes de preuve dans le contexte des communications électroniques,* Répertoire de droit pénal et de procédure pénale, Dalloz.

CONTE Philippe, *Terrorisme - Bas les masques !* JurisClasseur, Droit pénal n°6, Juin 2016, repère 6.

CONTE Philippe, *Minorité du sujet de l'image pornographique,* JurisClasseur, Droit pénal n°12, Décembre 2018.

CONTE Philippe, *Le divan d'Hercule,* JurisClasseur, Droit pénal n°3, mars 2019, repère 3.

CUTAJAR Chantal, *La loi pour la sécurité intérieure (principales dispositions)*, Recueil Dalloz 2003 p.1106.

DALLEST Jacques, *Un droit de réquisition consacré,* Dalloz AJ Pénal 2004 p.346.

DANIS-FATÔME Anne, *Lutte contre le terrorisme - La protection des données personnelles résiste à la surveillance générale qu'imposerait la lutte contre le terrorisme,* LexisNexis, Communication Commerce Electronique n°4, avril 2020.

DANIS-FATÔME Anne, *Opérateurs de téléphonie mobile – Pour la CEDH, la protection des données personnelles cède devant la nécessité d'assurer la sécurité publique*, LexisNexis, Communication Commerce Electronique n°5, mai 2020.

DAOUD Emmanuel et LEONE Thomas, *Fichiers Visabio et FAED : l'accès par une personne habilitée ne se présume pas et l'utilisation d'un mot de passe personnel n'est pas une garantie suffisante*, Dalloz IP/IT 2019 p.118

DAUTIEU Thomas, *La Commission Nationale de l'Informatique et des Libertés Saisine par les particuliers – Pouvoirs de contrôle et de sanction,* JurisClasseur Communication, Fasc. 4733.

DUMONT Jean, GEORGET Valérie et BONNET Audrey, *Fasc. 20 : Les nullités de l'information,* JurisClasseur Procédure pénale.

De COMBLES de NAYVES Pierre, *Le code de déverrouillage d'un téléphone n'est pas une convention de déchiffrement*, Dalloz AJ pénal 2019 p.439.

De LAMY Bertrand, *Procédure pénale - La constitutionnalisation de la procédure pénale*, LexisNexis Droit pénal n° 4, Avril 2019, dossier 3.

DECIMA Olivier, *La rupture du bracelet électronique et l'office du juge pénal,* Recueil Dalloz 2016 p.1538.

DECIMA Olivier, *Terreur et métamorphose*, Recueil Dalloz 2016, p. 1826.

DECIMA Olivier, *Du piratage informatique aux perquisitions et saisies numériques ?* Dalloz AJ pénal 2017 p.315.

DELBANO Fabrice, *Chapitre 332 – Pièces de procédure et Scellés,* Dalloz Droit de l'expertise, 2016.

DETRAZ Stéphane, *Vol de données informatiques,* Gazette du palais 18 juin 2015 n°169, p.8.

DUMENIL Gabriel, *La nécessité urgente d'encadrer procéduralement la mesure de cyber-infiltration,* LexisNexis, Droit pénal n°9, septembre 2018, étude n°22.

DUMENIL Gabriel, *Vers une dématérialisation du domicile : réflexions autour de la théorie du domicile virtuel en droit pénal,* LexisNexis, Droit pénal n° 7-8, Juillet 2019, étude n°17.

FAUCHER Pascal, *Juridictions de l'application des peines – Conditions de recevabilité, investigations, expertises, moyens de contraintes, procédure pénale,* JurisClasseur, Fasc. 30.

FERAL SCHUHL Christiane, *La collecte de la preuve en matière pénale,* AJ Pénal 2009.

FOURMENT François, *Nullités de l'instruction : un exemple de grief !* Gazette du Palais, 19 juillet 2016, n°271b0.

FOURMENT François, *Sécurité intérieure – La loi n°2017-258 du 28 février 2017 relative à la sécurité publique dans ses aspects de droit pénal,* LexisNexis, Droit pénal n°5, mai 2017.

FOURMENT François, *Détournement de procédure, fraude au champ d'application d'un pouvoir d'enquête ou d'instruction,* LexisNexis, Droit pénal n°9, Septembre 2019, comm. 156.

FRANSSEN Vanessa, *The European Commission's E-evidence Proposal: Toward an EU-wide Obligation for Service Providers to Cooperate with Law Enforcement?*, European Law Blog, 12 octobre 2018.

GRANGER Marc-Antoine, *La distinction police administrative / police judiciaire au sein de la jurisprudence constitutionnelle*, Dalloz RSC 2011 p.789.

GAUTRON Virginie, *Usages et mésusages des fichiers de police : la sécurité contre la sureté ?*, Dalloz AJ Pénal 2010 p.266.

GAUTRON Virginie, *Fichiers de police – Réglementation française,* Dalloz, Répertoire de droit pénal et de procédure pénale, mars 2019.

GOUTTENOIRE Adeline et FULCHIRON Hugues, *Autorité parentale – Titre 2 Exercice de l'autorité parentale,* Répertoire de droit civil, Dalloz, al. 304 et s.

HAUSER Jean, *Filiation – Identification génétique. – Procréation médicalement assistée*, JurisClasseur Code civil.

HENNION-JACQUET Patricia, *Précisions sur la régularité des actes d'enquête (citius, altius, fortius : oui, mais sans dopage)*, Recueil Dalloz 2013 p.2826.

HERRAN Thomas et LACAZE Marion, *Affirmation de la compétence du juge pénal dans le contrôle des perquisitions administratives,* Dalloz AJ pénal 2017 p.30.

JACOPIN Sylvain, *Le début d'une évolution sur la nature de la chose susceptible d'appropriation frauduleuse,* LexisNexis Droit pénal n°4, avril 2001, chron. 16.

JEANDIDIER Wilfrid, *Criminalité et délinquance organisées,* Dalloz répertoire de droit pénal et de procédure pénale.

JOUNIOT Sylvie, *Vol : avatars d'une infraction protéiforme*, Dalloz AJ pénal 2019.

LARRIBEAU-TERNEYRE Virginie, *La responsabilité de l'expert judiciaire; à l'ombre du droit commun de la responsabilité civile,* Les Petites Affiches, 2 déc. 1998, p.7.

LAURENT Benoît, ROTH Cyril, BARBIER Gildas, LABROUSSE Pascale, *Géolocalisation par suivi dynamique du téléphone portable : conditions de licéité au regard de l'article 8 de la Convention européenne des droits de l'homme*, Recueil Dalloz, 2014 p.311.

LAVRIC Sabrina, *Fichier EDVIGE : recours devant le Conseil d'Etat*, Recueil Dalloz 2008 p.2222.

LAVRIC Sabrina, *Fichiers de police : publication d'un rapport parlementaire*, Recueil Dalloz, 2009 p.938.

LENA Maud, *Les rapprochements judiciaires*, Dalloz AJ pénal 2017.

LEPAGE Agathe, *un an de droit pénal des nouvelles technologies (Octobre 2014 – Octobre 2015)*, LexisNexis, Droit pénal n°12, décembre 2015, chronique n°10.

LEPAGE Agathe, *Tel est pris qui croyait prendre… mais est sauvé par le principe de loyauté de la preuve,* Communication Commerce Electronique n°11, novembre 2016.

LEPAGE Agathe, *Enquête sous pseudonyme sur les réseaux numériques,* LexisNexis, Communication commerce électronique, avril 2018.

LEPAGE Agathe, *Contribution à l'interprétation de la notion d'apologie,* LexisNexis Communication Commerce Electronique n°9, sept. 2010, comm. 55.

LESCLOUS Vincent, *Chronique – Un an de droit de la garde à vue (1er juin 2010 - 1er juin 2011),* JurisClasseur Droit pénal n°9 Septembre 2011, chron. 7.

LETTERON Roseline, *Les débris de la loi « anti-casseurs »*, Dalloz AJ pénal 2019 p.259.

MARGAINE Clément, *La loi du 15 août 2014 et le milieu ouvert : vers un accroissement du contrôle des personnes condamnées*, Dalloz AJ pénal 2014.

MARON Albert et HAAS Marion, *Les oubliettes de la procédure,* LexisNexis, Droit pénal n°9, Septembre 2019, comm. 158.

MAROT Pierre-Yves, *Fonctions et mutations des fichiers de police*, Dalloz, AJ pénal 2007, p. 61.

MARTINELLE Mathieu, *L'utilisation des caractéristiques génétiques dans les procédures judiciaires,* Dalloz AJ pénal 2018 p.69.

MATHONNET Paul et GHNASSIA Michaël, *La Cour de cassation pose ses conditions en matière de réquisitions de documents délivrées au cours des enquêtes préliminaires*, Recueil Dalloz 2006 p.1429.

MAXWELL Winston et ZOLYNSKI Célia, *Protection des données personnelles*, Recueil Dalloz, 2019, p.1673.

MAYAUD Yves, *De la loi au Conseil constitutionnel, une réforme contrastée de la procédure pénale*, Dalloz, AJ pénal 2019, p. 176.

MEILLAN Eric, *Le renseignement intérieur : pour l'efficacité dans la démocratie*, LexisNexis, Droit pénal n°7-8, juillet 2016, étude 15.

MIANSONI Camille, *L'expertise pénale en enquête préliminaire et de flagrance. Le procureur de la République, prescripteur d'expertise*, Dalloz AJ Pénal 2011 p.564.

MICHALSKI Cédric, *La recherche et la saisie des preuves électroniques,* Gazette du Palais 11 fév. 2014 n°42 p.12.

MIGAYRON Serge, *Informatique – Pratique contentieuse. De l'information numérique à la preuve,* Communication Commerce Electronique n°4, avril 2017, LexisNexis.

MONTEIL Marine, *L'usurpation d'identité à l'épreuve du numérique*, Recueil Dalloz 2020 p.101.

MOURALIS Jean-Louis, *Preuve – Chapitre 3 – Recherche et appréciation des preuves,* Répertoire de droit civil, Dalloz, al. 557

MOUSTIERS Anaïs, *Preuve et biotechnologies : l'utilisation des empreintes génétiques à des fins judiciaires,* La preuve pénale sous la direction d'Olivier de FROUVILLE, La documentation Française.

NABAT Yoann, *Traitement automatisé de données personnelles - Lorsque la Cour européenne des droits de l'homme s'intéresse au fichage des manifestants... échos lointains de débats français*, LexisNexis Droit pénal n° 6, Juin 2019, comm. 116.

PELISSIER Pierre, *Circulation routière – Responsabilité pénale et poursuites*, Dalloz, Répertoire de droit pénal et de procédure pénale, mai 2019.

PELTIER Virginie, *Atteintes au secret des correspondances commises par les personnes dépositaires de l'autorité publique,* JurisClasseur Pénal Code art. 432-9, Fasc. 20.

PERRAY Romain, *Données à caractère personnel – Introduction générale et champ d'application de la loi "Informatique et libertés*, JurisClasseur Communication Fasc 930.

PERRIER Jean-Baptiste, *Les garanties de la procédure pénale dans la loi du 3 juin 2016 : entre illusion(s) et désillusion(s),* Recueil Dalloz 2016 p.2134.

PRADEL Jean, *Définition de la perquisition : notion de lieu clos,* Recueil Dalloz 1995 p.144.

PRONIER Julien, *Géolocalisation,* JurisClasseur Procédure pénale art. 230-32 à 230-44 Fasc. 20.

QUEMENER Myriam, *Les spécificités juridiques de la preuve numérique,* Dalloz AJ Pénal 2014 p.63.

QUEMENER Myriam, *Les dispositions liées au numérique de la loi du 3 juin 2016 renforçant la lutte contre le crime organisé et le terrorisme*, Dalloz IP/IT 2016 p.431.

QUEMENER Myriam, *Perquisitions et saisies de données informatiques dans le cadre de l'état d'urgence,* Dalloz IP/IT, 2016, p.499.

QUEMENER Myriam et DALLE Frédérique, *L'accès à la preuve numérique, enjeu majeur de toute enquête pénale : pratique et perspectives,* Dalloz IP/IT, 2018, p.418.

RASCHEL Evan, *Sécurité intérieure – La sécurité intérieure et la lutte contre le terrorisme entre cadence et décadence : commentaire de la loi n°2017-1510 du 30 octobre 2017*, LexisNexis, Droit pénal n°12, décembre 2017, étude n°23.

RIBEYRE Cédric, *LOPPSI II : de nouvelles règles au service de la répression,* LexisNexis, Droit pénal n° 7-8, Juillet 2011, étude 10.

RIBEYRE Cédric, *Loi n°2016-731 du 3 juin 2016 […] – Et maintenant ?* Droit pénal LexisNexis n°9, septembre 2016, étude 17.

RIBEYRE Cédric, *État d'urgence - État d'urgence et procédure pénale : le juge pénal compétent pour contrôler les perquisitions administratives,* LexisNexis, Droit pénal n° 3, Mars 2017, étude n°6.

ROBACZEWSKI Corinne, *atteinte aux systèmes de traitement automatisé de données*, JurisClasseur Pénal Code art. 432-9, Fasc. 20.

ROUMIER William, *Régime d'effacement des données du fichier d'antécédents judiciaires*, JurisClasseur Droit pénal n°9 Septembre 2018.

ROUSSEL Bruno, *Traitements de données à caractère personnel pour la cybersécurité : du difficile équilibre entre efficacité et respect des droits des salariés*, Lamy, Droit de l'immatériel, octobre 2018.

ROZENFED Sylvie, *Sécurité : La pomme de la discorde,* Expertises des systèmes d'information, mars 2016 n°411.

SAINT-PAU Jean-Christophe, *Loi Perben II - L'entraide judiciaire internationale et européenne*, LexisNexis Droit pénal n° 7/8, Juillet 2004, étude 9.

SAINT-PAU Jean-Christophe, *Les investigations numériques et le droit au respect de la vie privée,* Dalloz AJ pénal 2017, p.321.

SALATI Olivier, *Chapitre 121 – Liste nationale des experts judiciaires et listes dressées par chaque cour d'appel,* Dalloz Droit de l'expertise, 2016.

SCHWENDENER Marc, *Police technique et scientifique*, Dalloz Répertoire de droit pénal et de procédure pénale, février 2019.

SONTAG KOENIG Sophie, *Les perquisitions 2.0 : quand l'informatique se saisit de l'immatériel,* Dalloz AJ Pénal 2016 p.238.

SOURISSEAU Yann, *La poursuite des réseaux de prostitution*, Dalloz AJ Pénal 2012 p.201.

PY Bruno, *Secret professionnel – Opposition du secret*, Dalloz Répertoire de droit pénal et de procédure pénale, Février 2017.

THOMAS-TAILLANDIER Delphine, *Le nouveau fichier national des auteurs d'infractions terroristes*, Dalloz AJ pénal 2015.

VEDEL Renaud, *Le rôle des fichiers dans l'action opérationnelle des services de sécurité intérieure*, Dalloz AJ pénal 2007.

VERGES Etienne, *Réforme de la procédure pénale : une loi fleuve, pour une justice au gré des courants. A propos de la loi n°2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice*, LexisNexis, Droit pénal n°5, mai 2019, étude 12.

VERNY Edouard, *La responsabilité pénale au sein de l'équipe médicale,* Dalloz, Revue de Droit Sanitaire et Social, 2008, p.58.

VERNY Edouard, *Usurpation d'identité,* JurisClasseur Communication, Fasc. 58.

VIBRAC Geoffrey, *Les fichiers à l'épreuve de nouveaux droits effectifs pour les personnes ?*, Dalloz AJ pénal 2018 p.564.

VOLFF Jean, *Elaborer et mener la politique pénale d'un parquet*, Recueil Dalloz 2009 p.317.

C. Colloques

DECIMA Olivier, *Les investigations numériques en procédure pénale française : du piratage informatique aux perquisitions et saisies numériques ?* Colloque sur « les investigations numériques en procédure pénale comparée » du 5 mai 2017 au pôle juridique et judiciaire de Bordeaux.

JAEGER Christian, *Enquêtes secrètes, perquisitions en ligne et conservation des données en Allemagne : un équilibre entre les intérêts de la poursuite pénale et les garanties de l'Etat de droit,* Colloque sur « les investigations numériques en procédure pénale comparée » du 5 mai 2017 au Pôle Juridique et Judiciaire de Bordeaux.

PELTIER Virginie, *Les écoutes judiciaires en procédure pénale : « Les preuves obtenues par IMSI-catchers et les droits fondamentaux »,* Les colloques de l'ISCJ n°2, octobre 2017.

RIBEYRE Cédric, *Les écoutes judiciaires en procédure pénale : « Ecoutes et secret professionnel des avocats : le point de vue de l'universitaire »,* Les colloques de l'ISCJ n°2, octobre 2017.

ROUCOU Denis (premier vice-président en charge du service pénal au TGI de Bordeaux), *Les écoutes judiciaires en procédure pénale : « Les problèmes juridiques posés par les nouveaux modes d'écoutes, le point de vue des magistrats »,* Les colloques de l'ISCJ n°2, octobre 2017.

D. Décisions, avis, traités, rapports

Divers

ARCEP, *Observatoire des marchés des communications électroniques*, 2 août 2018.

BATHO Delphine et BENISTI Jacques-Alain, *rapport d'information sur les fichiers de police,* Commission des lois constitutionnelles, de la législation et de l'administration générale de la République de l'Assemblée Nationale, enregistré le 24 mars 2009.

BATHO Delphine et BENISTI Jacques-Alain, *rapport d'information sur la mise en œuvre des conclusions de la mission d'information sur les fichiers de police,* Commission des lois constitutionnelles, de la législation et de l'administration générale de la République de l'Assemblée Nationale, enregistré le 21 décembre 2011.

BAUER Alain, *Rapport public - Fichiers de police et de gendarmerie : comment améliorer leur contrôle et leur gestion ?*, 27 nov. 2006.

IMBERT-QUARETTA Mireille, *1er rapport d'activité, La centralisation des interceptions judiciaires*, mai 2017.

Ministère de la justice du Quebec, bureau de la sous-ministre et sous-procureure générale, *Plan directeur en ressources informationnelles du ministère*, 17 décembre 2019.

PARIS Didier et MOREL-A-L'HUISSIER Pierre, *Rapport d'information sur les fichiers mis à la disposition des forces de sécurité*, déposé et enregistré à l'Assemblée nationale le 17 octobre 2018.

Commission Nationale de l'Informatique et des Libertés

Conclusions du contrôle du système de traitement des infractions constatées (STIC), Rapport remis au Premier ministre le 20 janvier 2009.

Délibération n°2009-355 du 11 juin 2009 portant avis sur un projet de décret en Conseil d'Etat portant création de l'application relative à la prévention des atteintes à la sécurité publique (saisine n° AV 08023079).

Délibération 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 n°2010-117 du 6 mai 2010 portant avis sur le projet d'arrêté autorisant la mise en œuvre d'un traitement automatisé de données à caractère personnel dénommé « Gestion des amendes forfaitaires des unités élémentaires de la gendarmerie départementale et des gendarmeries spécialisées » qui émet un avis sur l'application PULSAR.

Délibération n°2011-233 du 21 juillet 2011 portant avis sur un projet de décret en Conseil d'Etat renforçant l'efficacité et la sécurité du bureau d'ordre national automatisé des procédures judiciaires dénommé « Cassiopée ».

Délibération 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°2011-420 du 15 décembre 2011 portant avis sur un complément au projet de décret en Conseil d'Etat renforçant l'efficacité et la sécurité du bureau d'ordre national automatisé des procédures judiciaires dénommé « Cassiopée ».

Fiche « ANACRIM : logiciels de rapprochement judiciaire à des fins d'analyse criminelle » du 8 avril 2014.

Ministère de la Justice, *Projet de loi de programmation 2018-2022 et de réforme pour la justice – Rapport Annexe*, 23 avril 2018

Norme Simplifiée n°48 relative aux « Fichiers clients-prospects et vente en ligne ».

Rapport adopté en séance plénière le 13 juin 2013 : conclusions du contrôle des fichiers d'antécédents du ministère de l'intérieur.

Union Européenne

Conférence européenne de lutte contre le terrorisme, *Déclaration commune de sept ministres européens,* Paris, 5 novembre 2018.

Convention européenne de sauvegarde des droits de l'homme.

Convention de Budapest sur la cybercriminalité du 23 novembre 2001 Rapport explicatif de la Convention de Budapest (www .europea.eu).

Décision 2008/615/JAI du Conseil du 23 juin 2008 relative à l'approfondissement de la coopération transfrontalière, notamment en vue de lutter contre le terrorisme et la criminalité transfrontalière.

Protocole additionnel à la Convention sur la cybercriminalité, relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques, 28 janvier 2003

Rapport explicatif du Protocole additionnel à la Convention sur la cybercriminalité, relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques, 28 janvier 2003.

Conseil Justice et affaires intérieures : compte-rendu de la réunion des 8 et 9 juin 2017 (Source : www.consilium.europa.eu/fr/meetings/jha/2017/06/08-09/)

Conseil Justice et affaires intérieures : compte-rendu de la réunion des 12 et 13 octobre 2017 (Source : www.consilium.europa.eu).

Conseil Justice et affaires intérieures : compte-rendu de la réunion des 7 et 8 octobre 2019 (Source : www.consilium.europa.eu).

Accords internationaux

Traité d'entraide judiciaire en matière pénale signé le 10 décembre 1998 entre la France et les Etats-Unis d'Amérique.

Convention d'entraide judiciaire en matière pénale entre la France et l'Afrique du Sud du 31 mai 2001.

US-EU MLAT : accord entre l'Union européenne et les États-Unis d'Amérique en matière d'entraide judiciaire du 19 juillet 2003.

Instrument relatif à l'application du traité d'entraide judiciaire en matière pénale signé le 10 décembre 1998 entre la France et les Etats-Unis d'Amérique, signé à La Haye le 30 septembre 2004.

IV – Thèses

AYADI Rim, *Théorie pour la réforme de la procédure pénale : éléments pour une définition juridique de la réforme*, soutenue le 12 décembre 2011 à Montpellier 1.

DEMARCHI Jean-Raphaël, *Les preuves scientifiques et le procès pénal*, LGDJ, 2012. Thèse soutenue en 2010 à Nice.

FARGEAUD Pierre, *La preuve informatique en droit français : les aspects juridiques de l'inforensique,* soutenue en 2007 à Limoges.

FIORINI Benjamin, *L'enquête pénale privée, Etude comparée des droits français et américain, Institut Universitaire Varenne*, Collection des Thèses, 2018.

FUHR Thomas, *Conception, preuves et analyse de fonctions de hachage cryptographiques,* le 3 octobre 2011.

HENNEQUIN Shirley, *La preuve numérique dans le procès pénal,* soutenue en 2011 à Aix-Marseille.

HENNION Patricia, *Preuve pénale et droits de l'Homme*, soutenue le 19 décembre 1998 à Nice-Sophia Antipolis

JOSSERAND Sylvie, *L'impartialité du magistrat en procédure pénale*, soutenue en 1996 à Grenoble 2.

MILOUDI Farouk, *Le procureur de la République et la procédure judiciaire*, soutenue en 2010 à Nice.

POTASZKIN Tatiana, *L'éclatement de la procédure pénale : vers un nouvel ordre procédural pénal ?*, soutenue en 2009 à Toulouse1 Capitole.

SONTAG KOENIG Sophie, *Technologies de l'information et de la communication et défense pénale*, soutenue le 13 décembre 2013, publiée aux Editions mare et martin, 2015.

TOUILLIER Marc, *Procédure pénale de droit commun et procédures pénales spéciales,* soutenue le 30 novembre 2012 à Montpellier 1.

TOURE Aminata, *L'influence des nouvelles technologies dans l'administration de la justice pénale,* soutenue le 8 décembre 2015.

V – Entretiens

AKZOY RETONAZ Eylem, Maître de conférences à l'université de Galatasaray, le 5 mai 2017.

BOUISSET Karline, juge d'instruction au Tribunal de Grande Instance d'Albi, 2008.

CRASNIER Fabrice, Responsable du pôle Forensic, SCASSI, le 1er décembre 2017.

IMBERT-QUARETTA Mireille, le 27 septembre 2017.

NEYRAND Gilles, secrétaire général au Parquet général – Cour d'Appel de Toulouse, le 20 janvier 2016.

TONELLI Stéphane, Chef du groupe cybercriminalité, Section de Recherches de Toulouse, Gendarmerie Nationale, le 1er décembre 2017.

VI – Jurisprudences

Juridictions judiciaires

Crim. 10 déc. 1968 n°68-92.02, Bull. crim. 1968 n°333.

Crim. 9 mars 1981 n°80-93.646, Bull. crim. 1981 n°86.

Crim. 1er déc. 1987 n°87-85.270 : JurisData n° 987-002030.

Crim. 7 juin 1988 n°88-81828, Bull. crim. 1988 n°258.

Crim. 12 janv. 1989, Bull. crim. 1989 n°14.

Crim. 10 mars 1993 n°91-80.936 : JurisData n° 1993-704828.

Crim. 29 sept. 1993 n°92-86.589 : JurisData n°1993-002565.

Crim. 11 janv. 1994 n°93-84.837, Bull. crim. 1994 n°15.

Crim. 29 mars 1994 n°93-84.995 : Bull. crim. 1994 n° 118 p.259.

Crim. 19 sept. 1994 n°93-85.641 : JurisData n°1994-001996.

Crim. 27 mars 1995 n° 94-85.074, Bull. crim. 1995 n°127.

Crim. 10 dec. 1996 n°96-80.833 : JurisData n°1996-005199.

Crim. 15 janv. 1997 n°96-83.753 : Bull. crim. 1997 n°14.

Cim. 21 mai 1997 n° 95-84.050 : JurisData n°1997-003237.

Crim. 16 fev. 2000 n°99-86.307, Bull. crim. 2000 n°72.

Crim 27 fev. 2001 n°00-86.747, Bull. crim. 2001 n°50.

Crim. 22 Mai 2002 n°01-86.184 : JurisData n°2002-015314.

Crim. 18 juin 2002 n°01-86.098 ; Bull. crim. n°136.

Crim. 8 juill. 2004 n°04-80.145 ; Bull. crim. n°180.

Crim. 14 sept. 2005 n°05-84.021 ; Bull. crim. n°226.

Crim. 6 dec. 2005 n°05-85.076 ; Bull. crim. n°319.

Crim. 16 dec. 2005 n°15-82.643.

Crim. 23 mai 2006 n°06-81.705.

Crim. 20 mars 2007 n° 06-89.250 : JurisData n°2007-038316.

Crim. 3 avr. 2007 n°06-87.264 : JurisData n°2007-038631.

Crim. 3 avr. 2007 n°07-80.807 : JurisData n°2007-038632.

Crim. 3 oct. 2007 n°07-81.045 : JurisData n°2007-040853.

Crim. 4 dec. 2007 n°07-87.047 : JurisData n°2007-042022.

Crim. 15 septembre 2009 n° 09-82.597 ; Bull. crim. 2009 n°155.

Crim. 19 dec. 2007 n°07-86.885 : JurisData n°2007-042162.

Crim. 16 fév. 2011 n°10-82.865 : JurisData n°2011-003741.

Crim. 21 juin 2011 n°11-81.846 : JurisData n°2011-014804.

Crim. 9 nov. 2011 n°11-84.315 : JurisData n°2011-028835.

Crim. 22 nov. 2011 n°11-84.308 : JurisData n° 2011-026053.

Crim. 7 mars 2012 n°11-88.118

Crim. 28 mars 2012 n°11-83.012

Crim. 7 mai 2012 n°01-80.317 : JurisData n°2002-015312.

Crim. 5 fév. 2013 n° 12-80.573

Crim. 6 mars 2013 n° 12-87.810 : JurisData n°2013-004870.

Crim. 16 avril 2013 n°09-82.944.

Crim. 22 oct. 2013 n°13-81.945 ; Bull. crim. 2013, n°196.

Crim. 22 oct. 2013 n°13-81.949 ; Bull. Crim. 2013 n°197.

Crim. 6 nov. 2013 n°12-87.130 : JurisData n°2013-024912.

Crim. 17 sept. 2014 n°13-87.164.

Crim. 30 sept. 2014 n°14-84.834 : JurisData n°2014-022705.

Crim. 3 mars 2015, n° 14-80.415 : JurisData n°2015-004059

Crim. 8 juillet 2015 n°15-81.731 : JurisData n°2015-016435

Crim. 20 mai 2015 n°14-81.336 : JurisData n°2015-011834.

Crim. 14 oct. 2015 n°14-83.300.
Crim. 17 nov. 2015 n°15-84.025 : JurisData n°2015-025735.
Crim. 24 nov. 2015 n°14-87.689.
Crim. 9 déc. 2015 n°14-87.835 : JurisData n°2015-027585.
Crim. 9 fév. 2016 n°15-85.069 : Jurisdata n°2016-001953.
Crim. 9 fev. 2016 n°15-85.071.
Crim. 30 mars 2016 n°15-86.693, Bull. crim. 2016, n°110.
Crim.10 mai 2016 n°15-87.713, Bull. crim. 2016, n°850.
Crim. 10 mai 2016 n°16-80.312.
Crim. 7 juin 2016 n°15-87.755 : JurisData n°2016-011071.
Crim. 15 juin 2016 n°15-86.043 : Bull crim. 2016, n° 186.
Crim. 6 sept. 2016 n° 15-84.963.
Crim. 11 oct. 2016 n°09-88.080.
Crim. 2 nov. 2016 n°16-82.376 : JurisData n°2016-022725.
Crim. 2 nov. 2016 n°16-81.539 : JurisData n°2016-022750.
Crim. 3 nov. 2016 n° 15-82.191.
Crim. 13 déc. 2016 n°16-82.176 : JurisData n°2016-026322.
Crim. 13 déc. 2016 n° 16-84.794 : JurisData n°2016-026324.
Crim. 3 mai 2017 n°16-86.155 : JurisData n°2017-008272.
Crim. 23 mai 2017 n°16-87.323 : JurisData n°2017-009925.
Crim. 28 juin 2017 n°16-81.113 : JurisData n°2017-012975.
Crim. 6 février 2018 n°17-84.380 ; B. n°48.
Crim. 27 mars 2018 n°17-85.603 : JurisData n°2018-004696.
Crim. 10 avril 2018 n°17-85.607 : JurisData n°2018-005644.
Crim. 20 juin 2018 n°17-86.657 : JurisData n°2018-010675
Crim. 25 juillet 2018 n°18-80.651 : JurisData n°2018-014001
Crim. 22 août 2018, n°18-80.431, QPC.
Crim. 8 janv. 2019 n°18-80.748.
Crim. 4 juin 2019, n°18-85.042
Crim. 16 janv. 2019, n°18-86.127.
Crim. 19 février 2019 n°18-84.671 : Bull. crim. 2019 n°38.
Crim. 18 juin 2019 n°18-86.421 : JurisData n°2019-010513.
Crim. 18 juin 2019 n°19-80.015 : JurisData n°2019-010591.
Crim. 3 sept. 2019, n°19-80.164.
Crim. 18 sept. 2019, n°18-84.752.

Crim. 24 sept. 2019, n°18-85.736 : JurisData n°2019-016683.
Crim. 20 nov. 2019 n°18-83.541 : JurisData n°2019-020807.
Crim. 24 mars 2020 n°19-86.706 : JurisData n°2020-004614.

Civ. 1ère 17 oct. 2018 n°17-16.852, ECLI:FR:CCASS:2018:C100961.

Ass. plén. 9 déc. 2019, n°18-86.797. ECLI:FR:CCASS:2019:AP00650.

CA Paris, 5 avr. 1994.
CA Paris, 17 déc. 2001 n° 00/07565.
CA Lyon 1 déc. 2010 n°08/01170.
CA Paris 5 oct. 2016 n°14/25251.
CA Bordeaux 1 juin 2017 arrêt n°479, dossier n°17/00557
CA Paris 16 avril 2019, n°19/09267.

Juridictions administratives
Trib. admin. Montreuil, 8ème ch., 27 mai 2016, n°1500040.
CAA Marseille, 7ème ch., 30 mars 2018, n° 16MA02755.

T. conf. 8 oct. 2018, n°4134, M. G. c/ ministère de la Justice.

CEDH
CEDH 24 août 1998 Lambert c. France
CEDH 28 janvier 2003 Peck c. Royaume Uni
CEDH 6 juin 2006 Segerstedt-Wiberg c. Suède
CEDH 3 avril 2007 Copland C. Royaume Uni
CEDH 4 dec. 2008 S. et Marper c. Royaume Uni
CEDH 23 novembre 2010 Moulin c. France
CEDH 18 avril 2013 M. K. c. France
CEDH 22 juin 2017 Aycaguer c. France
CEDH 30 janv. 2020 Breyer c. Allemagne

CJUE

CJUE 30 mai 2006, aff. C-317/04 et C-318-04 « Parlement contre Conseil »

CJUE 8 avril 2014, aff. C293/12 et C594/12 « Digital Rights Irland Ltd et a. c. Minister for communications »

CJUE 6 oct. 2015, aff. C-362/14 « Schrems »

CJUE 21 déc. 2016, aff. C-203/15 et C-698/15 « Tele2 Sverige et Watson »

CJUE 2 oct. 2018, aff. C-207/16 « Ministerio Fiscal »

Conseil constitutionnel

Conseil constitutionnel, décision n°2011-625 DC du 10 mars 2011

Conseil constitutionnel, décision n°2017-670 QPC du 27 octobre 2017

Conseil constitutionnel, décision n°2017-680 QPC du 8 décembre 2017

Conseil constitutionnel, décision n°2017-682 QPC du 15 décembre 2017

Conseil constitutionnel, décision n°2018-696 QPC du 30 mars 2018

Conseil constitutionnel, décision n°2019-778 DC du 21 mars 2019

Conseil constitutionnel, décision n°2020-845 QPC du 19 juin 2020

INDEX ALPHABETIQUE

(Les chiffres renvoient aux numéros des pages)

J

L

N

P

R

S

T

U

V

TABLE DES MATIERES

Titre : Les investigations numériques en procédure pénale

Résumé :

Dans le contexte de numérisation que connaît notre société, l'enquête pénale doit s'adapter à la dématérialisation des investigations qui doivent permettre d'accéder, de collecter et de générer des données informatiques.
En l'état actuel de la procédure pénale, les informations numériques manipulées lors des actes d'enquête sont éparpillées et cloisonnées, ce qui nuit à l'efficacité de leur exploitation ainsi qu'à la protection des droits des personnes concernées par les données ainsi collectées ou générées.
La présente étude propose une analyse de toutes les informations numériques regroupées, qui sont recueillies au cours d'une procédure.
Les nombreux traitements de données à caractère personnel mis en œuvre par l'Etat et pour lesquels un accès est directement prévu lors de l'enquête pénale sont également éparpillés et physiquement séparés.
Loin de garantir une protection des droits des personnes fichées, cette séparation nuit à la qualité des données enregistrées et neutralise les possibilités de contrôles efficaces sur ces traitements. Une mise en commun mesurée de certaines données identiques est présentée ici : elle serait une source d'amélioration importante.

Mots clés : Dématérialisation de l'enquête pénale – Fichiers de police – Consolidation des données

---

Title : Digital investigations in french criminal procedure

Abstract :

Digitalization has more effects on our society. So, the criminal inquiry must be adapted in order to include digital investigations. Those investigations allow accessing, gathering and creating data.
In the current state of criminal proceedings in France, the digital information manipulated during investigative acts is separated, which undermines the efficiency of their exploitation as well as the protection of data subjects ' rights. This study proposes an approach that allows the analysis of all the digital information collected during a procedure, grouped, for better exploitation.
Moreover, a lot of legal processing of personal data exist in France. Data recorded in those files are divided, and the same data is stored in many judicial files. Our work studies the possibility to aggregate some of the identical data, like identification or address in order to improve criminal proceedings.

Keywords : Digital forensic – Legal processing of personal data – Investigations on data gathered

---

Unités de recherche

Institut de Sciences Criminelles et de la Justice, ISCJ – EA 4633
Institut de Recherche en Informatique de Toulouse, IRIT – UMR 5505