Les technologies numériques comme nouveaux moyens au service des enquêteurs et de l'État

Émilie Gay

AIX-MARSEILLE UNIVERSITE
FACULTE DE DROIT ET DE SCIENCE POLITIQUE

MASTER 2 « LUTTE CONTRE L'INSECURITE »

LES TECHNOLOGIES NUMERIQUES COMME NOUVEAUX MOYENS AU SERVICE DES ENQUETEURS ET DE L'ETAT

Présenté et soutenu par

GAY EMILIE

Directeur de recherche : Monsieur Xavier Leonetti

- Année 2021/2022 -

« La Faculté n’entend donner ni approbation ni improbation aux opinions émises dans ce mémoire, qui doivent être considérées comme propres à leur auteur. »

Remerciements

Je tiens à remercier mon directeur de mémoire, Monsieur Xavier Leonetti, pour m'avoir soutenue et accompagnée dans l'élaboration de mon mémoire et d'avoir été particulièrement à l'écoute lorsque je lui exposais mes interrogations.

Je souhaite également remercier mon directeur de master, Monsieur Jean-Baptiste Perrier, pour m'avoir offert l'opportunité d'effectuer cette année enrichissante.

Abréviations

CNIL : Commission Nationale de l'Informatique et des Libertés

ANTENJ : Agence Nationale des Techniques d'Enquêtes Numériques Judicaires

PNIJ : Plate-forme nationale des interceptions judiciaires

LINC : Laboratoire d'Innovation Numérique de la CNIL

OCDE : Organisation de coopération et de développement économiques

ONU : L'Organisation des Nations unies

CPP : Code de procédure pénale

CSI : Code de sécurité intérieure

IA : Intelligence Artificielle

GAFI : Groupe d'action financières

D. : Recueil Dalloz

JCP G : La semaine juridique, édition générale

AJ Pénal : Actualité juridique Pénal

Droit pénal : Revue Droit pénal, LexisNexis

Gaz. Pal. : Gazette du Palais

RSC : Revue de science criminelle et de droit pénal comparé

RPDP : Revue pénitentiaire et de droit pénal

Sommaire

Introduction

« *Les données explosent et sont devenues les pépites du 21ème siècle. Cette nouvelle dimension bouleverse le travail des forces de l'ordre et des services d'enquêtes* »[1].

L'objectif de ce mémoire sera d'étudier le recours au technologies numériques dans la lutte contre la délinquance, à la fois par les services d'enquêtes limités par un cadre législatif et par les citoyens qui, eux, n'hésitent pas à s'affranchir de ce droit.

Pour comprendre et déterminer les enjeux du développement des techniques modernes d'enquêtes, il est important d'appréhender les technologies numériques. La notion de « technologies numériques » doit tout d'abord être dissociée pour être comprise dans son ensemble. Le terme de « technologies » est défini comme un « Ensemble cohérent de savoirs et de pratiques dans un certain domaine technique, fondé sur des principes scientifiques »[2].

Ensuite, le terme numérique a été initialement employé pour désigner la technique d'enregistrement de sons, d'images et de vidéos en opposition à l'analogique[3]. L'enregistrement analogique reproduit un son de manière analogue à la réalité c'est-à-dire en reproduisant la continuité de l'onde sonore sur un support[4]. L'objectif du numérique quant à lui est de discrétiser le continu de l'information (son, image…). On appelle cela un « échantillonnage » : après avoir choisi des échantillons de l'onde sonore, on va seulement considérer les changements qui interviennent à intervalles déterminés et non l'ensemble de l'information.

Ces dernières décennies, les avancées technologiques ont permis de révolutionner notre quotidien et la signification du mot « numérique » n'est plus utilisé dans le sens mathématique du terme. Aujourd'hui, l'expression de « technologies numériques » est généralement employée au sujet des hautes technologies mais plus précisément des nouvelles technologies de l'information et de la communication. Utilisée pour désigner une

[1] Deveryware, « La data au cœur de l'enquête », Livre blanc, octobre 2020

[2] Larousse, Définition technologie, https://www.larousse.fr/dictionnaires/francais/technologie/76961

[3] Marcello Vitali-Rosati, Pour une définition du « numérique », https://louisderrac.com/wp-content/uploads/2019/09/Pour-une-definition-du-numerique_Vitali-Rosati.pdf

[4] Bis 3

alliance entre les télécommunications de l'informatique, elle s'est répandue par le biais de l'information audiovisuelle.

Contrairement aux données chiffrées qui, avant le développement du web, transitaient majoritairement par les réseaux, l'information audiovisuelle permet de faire transiter des images et sons. Ces données sont beaucoup plus volumineuses que les précédentes, en raison du développement massif, après 1990, des infrastructures de télécommunication ainsi que des réseaux à haut débit[5]. Ce dernier a permis la transmission de quantités importantes d'informations, et ce, de façon plus fluide et rapide.

Dans cet ordre d'idée, la signification de l'expression « technologies numériques » doit être entendue comme un ensemble de savoirs et de pratiques fondés sur un système binaire dont l'objectif est de faciliter la qualité de vie humaine[6].

Ainsi, les avancées technologiques des dernières décennies ont permis le développement de nombreux appareils électroniques tels que les téléphones, les ordinateurs, les médicaments et beaucoup d'autres qui nous ont fait entrer dans une nouvelle ère. Le domaine du numérique regroupe ainsi plusieurs disciplines différentes telles que les sciences de l'information, de gestion, les sciences humaines, sociales et de l'informatique.

En revanche, le sens strict du terme « numérique » ne permet pas d'expliquer la généralisation de son emploi dans le langage commun. En effet, le développement massif des technologies de l'information et de la communication se comprend à la fois par la diversité des informations, l'importance de l'étendue de ses fonctions ainsi que l'accessibilité par les utilisateurs de ces informations. Les défis technologiques relevant des données numériques ont amené les scientifiques et les chercheurs à modifier leur façon de voir et d'analyser le monde.

Ainsi, lorsque sont apparus de nouveaux ordres de grandeur relatifs au partage, à la recherche, l'analyse des données, la notion de « Big Data » est née. Ce terme signifie, de traduction littérale, « grosses données » ou « données massives ». Plus précisément, il

[5] Serge Braudo, Définition de NTIC (nouvelles technologies de l'information et de la communication), https://www.dictionnaire-juridique.com/definition/ntic-nouvelles-technologies-de-l-information-et-de-la-communication.php

[6] Octets de Vie, Exemples de technologie numérique et sa définition, https://vidabytes.com/fr/ejemplos-de-tecnologia-digital/#Definiendo_tecnologia_digital

correspond au stockage, au traitement et à la gestion de larges volumes de données produites sur internet.

Aujourd'hui, les caractéristiques du Big Data reposent autour du critère des 3 V : le Volume qui correspond à la quantité massive de données (en général plus de 100 téraoctets), la Variété qui se réfère à la nature diverse et importante des données disponibles (c'est-à-dire différents formats de données), et enfin la Vitesse se rapporte à la vitesse à laquelle les données sont reçues et traitées. A cette définition, ont été rajoutés deux caractéristiques supplémentaires : la Valeur tout d'abord qui correspond à la qualification des données et enfin la Véracité qui se définit comme la conformité des données à la réalité.

Désormais, grâce aux progrès de l'informatique, il est possible de travailler avec une grande variété de données. Ces données peuvent être caractérisées par des bases de données d'images, des fichiers audios, des vidéos ou encore du texte écrit.

Aujourd'hui, chaque action connectée produit des données numériques, que ce soit des messages envoyés depuis un téléphone, des vidéos partagées en ligne, des publications sur des réseaux sociaux tels qu'Instagram, Twitter ou encore Facebook. Ces données peuvent être personnelles, professionnelles ou institutionnelles et provenir des diverses sources d'information. Le propre de ces données à l'état brut est qu'elles ne peuvent pas être traitées par un cerveau humain. Il est donc essentiel de les transformer pour qu'une information « compréhensible » parvienne aux utilisateurs.

La révolution numérique par le Big Data a bouleversé des domaines entiers de la vie quotidienne. C'est un phénomène qui est aujourd'hui largement étudié. Les immenses quantités de données relatives au Big Data, structurées ou non, peuvent être utilisées aussi bien par les entreprises, les institutions publiques et même scientifiques dans le but de prendre des décisions plus éclairées sur le choix des stratégies à adopter. La théorie du Big Data est simple : on part du principe selon lequel plus on possède d'information sur une situation ou un sujet, plus la prédiction sur l'avenir sera fiable et, subséquemment, plus les connaissances le seront.

Son utilisation présente d'autres avantages tels que la réduction des coûts et la possibilité d'avoir des retours en temps réel. De plus, au temps du papier, seule une partie des décisions de la Cour de cassation était publiée. Les supports ne permettaient pas de stocker une telle quantité, additionnée aux décisions des juridictions de degrés inférieurs, en bibliothèque. La

démarche s'inscrit dès lors dans un mouvement large d'open data[7], initié par la loi dite « République numérique »[8], qui promeut la mise à disposition du public des données d'intérêt général et particulièrement celles produites par les administrations.

Si l'apparition du Big Data a eu de nombreuses conséquences bénéfiques, telle que la facilitation de la vie quotidienne, il a aussi engendré de nombreux inconvénients. Parmi eux, un nouveau phénomène de délinquance a fait son apparition : la cybercriminalité. Cette notion ne dispose pas de définition universelle mais plusieurs organismes ont été amenés à la définir.

Selon l'Organisation de coopération et de développement économiques (OCDE), la cybercriminalité peut être définie comme « tout comportement illégal ou contraire à l'éthique ou non autorisé qui concerne un traitement automatique de données et/ou de transmission de données ». L'Organisation des Nations unies (ONU), quant à elle, détermine ce phénomène comme « tout comportement illégal faisant intervenir des opérations électroniques qui visent la sécurité des systèmes informatiques et des données qu'ils traitent ». De manière plus générale, la cybercriminalité peut être définie comme « l'ensemble des infractions pénales commises via les réseaux informatiques »[9].

Le développement d'Internet a permis l'apparition de plusieurs couches appelées respectivement le surface web, le deep web et le dark web. Le premier correspond aux sites accessibles par tout internaute via un moteur de recherche. Le second recense les sites pour lesquels un accès spécifique est requis ou un mot de passe. Le dark web quant à lui regroupe un ensemble de sites cachés qui sont accessibles seulement par le biais d'un navigateur particulier. C'est à partir de ce dernier que les internautes peuvent avoir accès à des contenus illégaux comme la pédopornographie.

Assez tôt, en raison du caractère transfrontalier des cybermenaces, les Etats ont pris conscience de la nécessité de prévenir cette forme de délinquance au niveau international. C'est pourquoi dès 1996, le Conseil de l'Europe a souhaité créer un instrument juridique

[7] Donnée ouverte, librement accessible

[8] Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique

[9] Gérard Haas, « La cybercriminalité à la fois côté obscur et face cachée du Big Data », Dalloz, 2016, p.21, https://www-dalloz-fr.lama.univ-amu.fr/documentation/Document?id=DIPIT%2FCHRON%2F2015%2F0041&ctxt=0_YSR0MD1iaWcgZGF0YcKneCRzZj1zaW1wbGUtc2VhcmNo&ctxtl=0_cyRwYWdlTnVtPTHCp3MkdHJpZGF0ZT1GYWxzZcKncyRzb3J0PSNkZWZhdWx0X0Rlc2PCp3Mkc2xOYlBhZz0yMMKncyRpc2Fibz1UcnVlwqdzJHBhZ2luZz1UcnVlwqdzJG9uZ2xldD3Cp3MkZnJlZXNjb3BlPUZhbHNlwqdzJHdvSVM9RmFsc2XCp3Mkd29TUENIPUZhbHNlwqdzJGZsb3dNb2RlPUZhbHNlwqdzJGJxPcKncyRzZWFyY2hMYWJlbD3Cp3Mkc2VhcmNoQ2xhc3M9

contraignant en matière de cybercriminalité[10]. Le 25 mai 2001, la convention du Conseil de l'Europe a vu le jour et a été signée par la France le 23 novembre de la même année. Celle-ci s'articule autour de plusieurs missions principales : l'harmonisation des législations nationales relativement aux incriminations relevant de la convention, l'adaptation des moyens procéduraux à internet en veillant en parallèle au respect ainsi qu'à la garantie des droits et libertés individuelles et finalement, la conformité aux conventions européennes d'entraide et d'extradition judiciaire, afin que les États disposent de moyens d'actions rapides et efficaces[11].

La nécessité pour les Etats de légiférer au niveau international démontre que les dangers qui découlent du développement massif des nouvelles technologies doivent prioritairement être pris en charge mais aussi l'importance primordiale de sanctionner les infractions commises par le biais de ces plateformes numériques. En conséquent, la possibilité de doter les services de police de moyens adéquats pour lutter contre ce type de délinquance est apparue indispensable pour équilibrer les forces et permettre à l'Etat d'adapter la lutte contre cette délinquance moderne. C'est dans cette optique que les opportunités offertes par le big data et l'intelligence artificielle vont être exploitées.

Les technologies numériques recouvrent un périmètre très large qui n'est juridiquement pas strictement défini, comprenant notamment le droit de l'informatique, le droit d'internet, le droit du numérique et des télécommunications. Ainsi, cette modernisation de l'information et de la communication se retrouve au sein de nombreux domaines de droit dont les règles sont éparses.

Aujourd'hui, nous sommes entrés dans ce que l'on pourrait appeler « l'ère du numérique » dans laquelle le numérique à envahit les enquêtes policières. En effet, c'est à la fois les délinquants et les enquêteurs qui y sont confrontés quotidiennement, que l'investigation s'opère dans un « milieu numérique » ou bien qu'elle s'effectue avec des « outils numériques ».

---

[10] Frédérique CHOPIN, « Cybercriminalité », *Répertoire IP/IT et Communication*, Dalloz, 2020 https://www-dalloz-fr.lama.univ-amu.fr/documentation/Document?id=ENCY%2FIPIT%2FPENRUB000083&ctxt=0_YSR0MD1jeWJlcmNyaW1pbmFsaXTDqcKneCRzZj1zaW1wbGUtc2VhcmNo&ctxtl=0_cyRwYWdlTnVtPTHCp3MkdHJpZGF0ZT1GYWxzZcKncyRzb3J0PSNkZWZhdWx0X0Rlc2PCp3Mkc2xOYlBhZz0yMMKncyRpc2Fibz1UcnVlwqdzJHBhZ2luZz1UcnVlwqdzJG9uZ2xldD3Cp3MkZnJlZXNjb3BlPUZhbHNlwqdzJHdvSVM9RmFsc2XCp3Mkd29TUENIPUZhbHNlwqdzJGZsb3dNb2RlPUZhbHNlwqdzJGJxPcKncyRzZWFyY2hMYWJlbD3Cp3Mkc2VhcmNoQ2xhc3M9&scrll=ENCY%2FIPIT%2FPENRUB000083%2F2020-02%2FPARA%2F7

[11] Bis

Ces deux catégories doivent être distinguées. L'enquête dans un milieu numérique implique l'emploi de techniques spécifiques qui vont permettre aux enquêteurs d'investiguer sur des délinquants qui se servent des « avantages » procurés par les technologies de l'information et de la communication pour parvenir à leurs fins. Pour autant, il n'est pas nécessaire de refondre totalement la procédure pénale pour lutter contre ces nouvelles formes de délinquances mais il est possible de s'y adapter.

Les moyens numériques au service des enquêteurs impliquent en revanche des changements plus profonds. La révolution des capacités de traitement informatiques a rendu possible le traitement ainsi que le recoupement de données inaccessibles aux capacités intellectuelles humaines. Anacrim, un outil d'analyse criminelle de la Gendarmerie Nationale, a notamment permis de relancer l'affaire dite du « petit Grégory » vieille de plus de 30 ans et pour laquelle les enquêteurs étaient impuissants. En effet, en améliorant le traitement des procès-verbaux et des données telles que les appels téléphoniques et les informations bancaires, le logiciel a aidé les gendarmes à prouver l'implication de l'auteur du meurtre.

Les cadres de l'enquête judiciaire ont alors progressivement changé, pour parvenir à des règles de procédures dérogatoires en lien avec la délinquance et la criminalité organisée (comme le trafic de stupéfiant et la lutte contre le terrorisme). Ainsi, il existe dorénavant un dispositif légal autorisant une meilleure coercition des moyens d'enquête et, de cette manière, on assiste à une diversification des technologies numériques et des outils dont disposent les enquêteurs.

C'est cette seconde catégorie concernant « les moyens » employés qui va retenir notre attention au sein de ce mémoire. En effet, nous allons nous concentrer sur l'emploi de ces technologies numériques dans la lutte contre la criminalité sans s'attarder précisément sur l'environnement numérique.

L'article L111-1 du CSI prévoit que « La sécurité est un droit fondamental et l'une des conditions de l'exercice des libertés individuelles et collectives ». C'est pourquoi, parallèlement, est apparue la nécessité d'encadrer juridiquement l'utilisation des outils numériques au sein des enquêtes policières dans un but de protection des droits et libertés fondamentaux. Les risques d'atteintes se sont multipliés avec le développement du Big Data. En effet, l'une des grandes problématiques existantes depuis le développement du web concerne la confidentialité et le respect de la vie privée. Plus précisément, les faiblesses associées au Big Data sont la confidentialité des données, la sécurité des données stockées

en raison des risques d'espionnage numérique, mais aussi la manipulation des données délicates. La rapidité, la fluidité ainsi que la quantité d'informations pouvant être échangées entre des millions d'internautes en un instant a bien entendu créé des risques d'atteintes à la vie privée.

C'est la raison pour laquelle le législateur a été contraint de prévoir un encadrement juridique strict dans l'objectif de prévenir ces atteintes. L'une des législations pionnières en la matière fut la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés[12]. Ce texte a pour objectif « d'éviter ou de contrôler la constitution de fichiers directement ou indirectement nominatifs qui soient dangereux pour les personnes concernées du fait des informations recueillies et conservées, ou qui pourraient le devenir s'ils étaient détournés de leur finalité première. Sont naturellement soit interdits, soit soumis à déclaration préalable, la constitution de fichiers portant sur la vie privée, les opinions politiques, philosophiques ou religieuses, les mœurs ou encore l'état de santé »[13].

La surveillance de l'application adéquate de ce dessein a été confiée à la commission nationale de l'informatique et des libertés (CNIL), autorité administrative indépendante qui dispose d'un pouvoir de contrôle et de sanction créé spécialement pour y répondre. Sa mission est de veiller à ce que le développement de ces technologies modernes ne porte atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée ou encore aux libertés individuelles ou publiques[14].

Les enjeux sont nombreux et importants, au regard du double mouvement permanent de déconstruction puis reconstruction des normes législatives. En effet, le cyberespace a fait l'objet d'une inflation législative avec une succession de réformes législatives multipliant les règles de droit et les cadres juridiques. On se trouve aujourd'hui dans une course permanente entre l'évolution rapide et incessante des technologies numériques et la nécessité pour l'Etat d'encadrer leur utilisation pour préserver les libertés individuelles. Cette effervescence juridique a dégagé l'existence de deux problématiques majeures. La première est un phénomène qu'on pourrait qualifier « d'obsolescence » des textes de lois qui se caractérise par sa rapidité. Effectivement, le législateur est souvent contraint dans ce

[12] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

[13] François Pellegrini, Sébastien Canevet, « Le droit du numérique : une histoire à préserver », 2013 https://edutice.archives-ouvertes.fr/edutice-00940669/file/a1311e.htm

[14] Direction des affaires juridiques, « Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés », 06 janvier 1978 http://affairesjuridiques.aphp.fr/textes/loi-n-78-17-du-6-janvier-1978-relative-a-linformatique-aux-fichiers-et-aux-libertes/

domaine à numéroter les différentes versions des lois en raison de leur caractère successif. Tel est le cas des lois HADOPI[15] et LOPSSI[16] qui ont fait l'objet de deux versions successives par exemple.

Pour citer quelques exemples de cette inflation, se sont succédés des réformes concernant la création d'un droit sui generis dans un but de protection des producteurs de bases de données, la protection des programmes d'ordinateurs par le biais d'un droit d'auteur revisité, les mécanismes judiciaires et administratifs destinés à la lutte contre le partage illégal d'œuvres sous le contrôle de la Haute autorité pour la diffusion des œuvres et la protection des droits sur Internet, l'adaptation des règles en matière de preuve (la reconnaissance de la valeur de l'écrit électronique, l'encadrement de la signature électronique, la jurisprudence relative aux conditions techniques de validité des constats d'huissier en ligne…), la régulation des opérateurs de réseaux de communication sous l'égide de l'Autorité de régulation des communications électroniques et des postes[17].

Mais aussi relativement aux données à caractère personnel avec la refonte de la loi de 1978 en 2004 et ses décrets d'application. Les délibérations de la Commission Nationale de l'Informatique et des Libertés sur de nombreux sujets tels que la vidéosurveillance, la biométrie, les réseaux sociaux, les cookies, les données de connexion...) mais aussi la doctrine du G29, le groupe des CNIL européennes[18].

Nécessairement, la rapidité et la quantité de données pouvant être traitées par les logiciels de traitement de données ainsi que leur utilisation dans la vie quotidienne ont conduit l'Etat à intégrer certains outils numériques aux techniques d'enquêtes dans l'objectif d'améliorer les moyens de lutte contre la délinquance dont disposent les enquêteurs.

---

[15] Loi n°2009-669 du 12 juin 2009 favorisant la diffusion et la protection de la création sur Internet, dite « Hadopi 1 » puis la loi no 2009-1311 relative à la protection pénale de la propriété littéraire et artistique sur internet dite loi HADOPI 2.

[16] Loi n° 2002-1094 du 29 août 2002 d'orientation et de programmation pour la sécurité intérieure puis la loi n°2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure

[17] Jean-Baptiste Thomas-Sertillanges, « Droit et technologies : concilier l'inconciliable ? », *Réflexions épistémologiques pour un droit des libertés technologiques*, *Les Cahiers du numérique*, 2014, https://www.cairn.info/revue-les-cahiers-du-numerique-2014-2-page-17.htm

[18] Idem

Les éléments de preuves ont aussi dû être actualisés et réformés face à l'apparition d'une nouvelle discipline de procédure pénale : celle de la « preuve numérique ». C'est pourquoi, aujourd'hui, ce développement est devenu un défi pour le quotidien des enquêteurs judiciaires[19].

La révolution numérique a ainsi révolutionné la manière dont l'administration réalise ses missions dans le domaine de la sécurité. Vidéoprotection, radar de vitesse, portique de reconnaissance biométrique aux frontières sont autant d'innovations technologiques que les français ont vu apparaître depuis le début des années 2000 en la matière[20]. Ce n'est pourtant qu'une partie de ce que l'innovation permet de développer. Intelligence artificielle, robotique, biométrie, analyse de données massives, écoutes numériques représentent certains des domaines technologiques dont les progrès récents ont amené de nouvelle façon de les employer.

Cependant, de nombreux défis sont apparus dans le développement des enquêtes numériques à savoir notamment comment favoriser sa sauvegarde, empêcher son altération et sa falsification. De surplus, ces moyens d'investigation doivent s'adapter en raison de la menace qui envahit de plus en plus le numérique (menaces malware, ransomware, cybersécurité, fraude, faille de réseau…) et qui évolue elle-même avec l'apparition de nouvelles technologies telles que l'intelligence artificielle, la 5G ou encore le cloud. Enfin, ces moyens sont mis en difficultés par l'existence de défis humains que les enquêteurs doivent relever. Les données transitent désormais en très grosse quantité et de façon rapide ce qui implique nécessairement une quantité de travail subséquente aussi importante. Or, cette constatation entre en conflit avec les objectifs primordiaux de l'investigation que sont la rapidité et l'efficacité.

Cette assimilation des technologies numériques au sein des enquêtes judiciaires a permis à l'Etat d'apporter une réponse judiciaire plus rapide et efficace qu'auparavant. Les données sont ainsi devenues essentielles pour l'investigation.

---

[19] Eric OK, « La preuve numérique, Un défi pour l'enquête criminelle du 21e siècle », Les cahiers du numérique, https://www.cairn.info/revue-les-cahiers-du-numerique-2003-3-page-205.htm

[20] Basile Thodoroff, Arno Amabile, *Police numérique, une révolution sous surveillance* ?, Ecole des Mines, 2020

Plus récemment, est apparu une nouvelle technologie numérique d'ampleur : l'Intelligence artificielle (IA). Cette dernière se définit actuellement comme « l'ensemble de théories et de techniques mises en œuvre en vue de réaliser des machines capables de simuler l'intelligence ».[21] Selon Thomas Cassuto, conseiller à la cour d'Appel de Paris, le développement de l'Intelligence Artificielle (IA) repose à la fois sur la puissance de calcul, l'accès à des bases de données très vastes mais aussi sur les moyens de communication permettant les échanges de ces données et le traitement de celles-ci en réseau. Il affirme ainsi que « les nouvelles générations de processeur les réseaux neuronaux, l'intégration de la physique quantique ou encore les structures biologiques associées à l'électronique qui émergent peuvent se nourrir de bases de données gigantesques ». Elles sont alimentées par des objets connectés de plus en plus nombreux qui collectent une très grande quantité de données prenant en compte le consentement des utilisateurs de manière plus ou moins tacites[22].

A ce titre, une distinction doit être faite entre l'IA dite « faible » et l'IA dite « forte ». La première est capable d'effectuer des tâches spécifiques à partir d'un programme : il n'est ici pas question d'une conscience ni intelligence de la machine mais uniquement d'une forte spécialisation. C'est la catégorie d'IA qui est aujourd'hui employée à grande échelle. La seconde quant à elle (l'IA forte), fait partie des nombreuses « prophéties » de science-fiction littéraires et cinématographiques développées depuis longtemps. Il est ici question d'IA généraliste dotée d'une réelle intelligence qui lui permettrait d'éliminer l'espèce humaine[23].

Bien que nous n'en soyons pas encore arrivés à ce point, ces technologies permettent d'ores et déjà d'effectuer une analyse fine des comportements humains et ont pour objectif de prédire ou même suggérer leurs futurs actes. Le logiciel PredPol est un exemple de ces évolutions technologiques. En effet, auparavant employé par les services de police des Etats-Unis[24], il permet, selon les concepteurs, de prédire le lieu et l'heure d'un crime « jusqu'à 12 heures » avant la commission des faits, et ce, à partir de dix ans de procès-verbaux (type de crime, où et quand ils ont été commis...).

La principale différence entre le Big Data est l'Intelligence Artificielle se situe dans leur essence même. En effet, le premier, qui signifie métadonnées, se caractérise par des données

[21] Encyclopédie Larousse

[22] Thomas Cassuto, Droit et intelligence artificielle, 14 mars 2018, https://www.dalloz-actualite.fr/chronique/droit-et-intelligence-artificielle

[23] Mais nous n'en sommes pas encore arrivés à ce stade

[24] La police californienne a annoncé mettre un terme à ce programme en 2020 en raison d'une réallocation de ressources budgétaires pour la pandémie Covid-19.

à l'état brut qui, pour pouvoir être utilisées, doivent être préalablement nettoyées, structurées et intégrées. L'Intelligence Artificielle quant à elle constitue la « sortie », c'est-à-dire qu'elle résulte du traitement de ces données. Plus précisément, elle permet aux machines d'effectuer des fonctions cognitives à la manière des êtres humains. Elle agit sur la prise de décision qui effectue les missions d'un être humain de façon plus rapide et avec de moindres erreurs[25].

Selon Christiane Féral-Schuhl, auteur du livre Praxis Cyberdroit, de nouvelles technologies d'enquêtes se sont massivement développées dans le but d'identifier des suspects par le biais du réseau Internet. Les algorithmes sont une source considérable de possibilités de comparaison des données récoltées. Ils ont la particularité de faciliter grandement la conservation et l'exploitation de ces données notamment en croisant des informations.

Le fonctionnement de ces logiciels nécessite de collecter massivement des données. La difficulté se situe dans la nature de ces dernières. En effet, ce sont des données à caractère personnel voire des données sensibles qui vont être exploitées.

Il est nécessaire, avant la poursuite du raisonnement, de définir une donnée personnelle. Selon la CNIL, cette dernière est définie par « toute information se rapportant à une personne physique identifiée ou identifiable ». Suivant cette logique, une personne peut être identifiée directement c'est-à-dire par un nom ou un prénom mais aussi indirectement par exemple par un numéro de téléphone, une donnée biométrique ou encore des informations relatives à l'identité physique de l'individu. Ensuite, une personne peut être identifiée aussi bien à partir d'une donnée unique notamment par l'ADN mais aussi par le croisement de plusieurs données.[26]

Le traitement de ces données personnelles sur le territoire de l'Union Européenne est régi par le Règlement Général sur la Protection des Données (RGPD) (UE) 2016/679 du Parlement européen et du Conseil. Son périmètre d'application et les conséquences sous-jacentes quant à son application seront analysés plus loin.

[25] Devrum, « Comparaison entre l'intelligence artificielle et le Big Data », 2018, http://blog.devrun.com/l-article/comparaison-entre-l-intelligence-artificielle-et-le-big-data

[26] CNIL, « RGPD : de quoi parle-t-on ? », https://www.cnil.fr/fr/rgpd-de-quoi-parle-t-on

Concernant les logiciels dits « prédictifs », bien qu'ils soient d'ores et déjà opérationnels dans certains pays comme les Etats-Unis (nous y reviendrons plus tard), leur utilisation peut être disproportionnée par rapport au but poursuivi de sécurité publique des Etats. C'est pourquoi ce principe de proportionnalité est un enjeu de taille pour garantir le respect des libertés individuelles comme la protection de la vie privée et des données à caractère personnel.

Les dangers d'une utilisation abusive de ces algorithmes par les autorités ont connu une illustration en 2013. Edward Snowden, ex-consultant de la NSA, avait alors révélé publiquement l'existence du programme américain dénommé « PRISM ». Ce logiciel était un programme de surveillance électronique qui permettait à la NSA et au FBI de collecter des données à partir des grands acteurs d'internet tels que Microsoft et Google. Ces organismes pouvaient ainsi consulter toutes les informations désirées relatives aux utilisateurs. A la suite de ce scandale, le G29[27], un groupe de travail sur la protection des données et de la vie privée, a dénoncé l'illégalité que représentait cette « surveillance massive, systématique et sans distinction des citoyens européens » ajoutant que de « telles restrictions aux droits fondamentaux des citoyens européens ne sont pas acceptables dans une société démocratique » [28].

Une telle atteinte aux libertés fondamentales nous a permis de prendre conscience que l'utilisation des technologies numériques dans les enquêtes judiciaires doit être limitée au regard du respect des libertés individuelles, garantie primordiale dans un Etat de droit.

Enfin, parallèlement aux enquêtes policières, est apparu un nouveau phénomène : celui des enquêtes privées. Plus précisément, des citoyens de plus en plus nombreux ont fait le choix de mener des « enquêtes numériques » à l'image de la police pour lutter avec leurs propres moyens contre la délinquance. L'atout majeur dont ils disposent réside dans l'absence de réglementation juridique de ces enquêtes. Si les enquêteurs des services de police sont soumis à de nombreuses règles de procédures qui allongent et restreignent la résolution des

[27] G29 : Mis en place par l'article 29 de la directive du 24 octobre 1995 (95/46/CE) sur la protection des données et de la vie privée. Il comprend les CNIL nationales d'Europe.

[28] Christiane Féral-Schuhl, « Les enquêtes dans l'environnement numérique », *Praxis Cyberdroit*, 2020-2021, Titre 72, https://www-dalloz-fr.lama.univ-amu.fr/documentation/Document?id=DZ%2FPRAXIS%2FCYBERDROIT%2F2019%2FNIVO%2FL07-T72&ctxt=0_YSR0MD1iaWcgZGF0YSBldCBlbnF1w6p0ZXMgZGUgcG9saWNlwqd4JHNmPXNpbXBsZS1zZWFyY2g%3D&ctxtl=0_cyRwYWdlTnVtPTHCp3MkdHJpZGF0ZT1GYWxzZcKncyRzb3J0PSNkZWZhdWx0X0Rlc2PCp3Mkc2xOYlBhZz0yMMKncyRpc2Fibz1UcnVlwqdzJHBhZ2luZz1UcnVlwqdzJG9uZ2xldD3Cp3MkZnJlZXNjb3BlPUZhbHNlwqdzJHdvSVM9RmFsc2XCp3Mkd29TUENIPUZhbHNlwqdzJGZsb3dNb2RlPUZhbHNlwqdzJGJxPcKncyRzZWFyY2hMYWJlbD3Cp3Mkc2VhcmNoQ2xhc3M9&scrll=ANOTE_DZ%2FPRAXIS%2FCYBERDROIT%2F2019%2FPARA%2F72.05_1

affaires, ce n'est pas le cas des citoyens. Ces derniers, s'affranchissant de ces « règles », disposent de moyens bien plus étendus que l'Etat dans la conduite de leurs investigations.

Ces constatations amènent une autre interrogation essentielle qui sera la problématique étudiée au sein de ce mémoire :

Dans quelle mesure les technologies numériques peuvent-elles être un recours dans la lutte contre la criminalité ?

Pour répondre à cette question, nous nous concentrerons autour de deux axes principaux à savoir : les technologies numériques peuvent être mises au service de l'Etat et des enquêteurs comme moyens modernes de lutte contre la délinquance (I) mais aussi au service des citoyens qui, non soumis aux règles strictes qui gouvernent les enquêtes policières, s'affranchissent du droit pour mener des enquêtes privées (II).

Partie I. Les technologies numériques comme nouveaux moyens au service des enquêteurs et de l'état

Le développement du Big Data et de l'Intelligence artificielle a conduit l'Etat français à moderniser ses techniques d'enquêtes pour permettre une meilleure réponse judiciaire aux infractions (1). Ces nouvelles techniques d'enquêtes sont cependant limitées dans le contexte de notre Etat de Droit français et Européen (2) et ce, de façon plus stricte que dans certains pays.

Chapitre 1) Le Big Data et l'Intelligence Artificielle à disposition des services d'enquête

L'adaptation des technologies numériques aux techniques d'enquêtes judiciaires a permis à l'Etat de révolutionner ses méthodes de lutte contre la délinquance aussi bien en termes de rapidité que d'efficacité (section 1). Cependant, les évolutions dans ce domaine ont été fulgurantes ces dernières années, entraînant nécessairement des défis importants pour les enquêteurs (section 2).

Section 1) Une révolution des enquêtes judiciaires par le biais des nouvelles technologies

Le développement des techniques d'enquêtes au moyen des technologies numériques modernes représente des enjeux cruciaux dans la lutte contre la délinquance (§1). De cette manière l'arsenal juridique des enquêteurs policiers s'est trouvé révolutionné par l'apparition de nouveaux outils (§2).

§1 Les enjeux judiciaires de l'adaptation à ces nouveaux moyens

L'importance primordiale de l'adaptation des technologies modernes aux enquêtes de police se justifie par 2 raisons principales. Tout d'abord la nécessité pour l'Etat français de pouvoir faire face aux nouvelles formes de délinquances apparues à l'ère du numérique et dont l'évolution va de pair avec celle des technologies modernes. C'est aussi une manière de parvenir à perfectionner les techniques d'enquêtes judiciaires dans un monde où les technologies numériques font partie intégrante de la vie des individus.

Les investigations menées sur les infractions traditionnelles telles qu'elles existaient avant le développement du numérique permettaient aux enquêteurs de relever des indices sur des scènes matérielles et engendraient un travail long et considérable pour résoudre des affaires complexes, le manque de preuves fiables et intangibles se trouvant être un frein important.

En effet, si l'ADN ou les traces papillaires retrouvées sur une scène de crime permettent d'établir avec certitude la présence d'un individu sur les lieux, il est nécessaire d'avoir en sa possession cet ADN et ces traces pour pouvoir les comparer. Si tel n'est pas le cas, le code de procédure pénale (CPP) prévoit, sous certaines conditions, l'enregistrement des traces prélevées dans les fichiers de police ou gendarmerie tels quel que le FAED[29] ou le FNAEG[30]. Est également recherchée la présence de délinquants dans les fichiers comparés, cependant, dans la plupart des cas cela n'aboutira pas au résultat escompté. En effet, nombreuses sont les traces et infractions qui conservent le statut d'auteur inconnu.

C'est pourquoi les technologies modernes présentent des apports majeurs dans la lutte contre la délinquance. Premièrement, les délinquants évoluent désormais au sein de cadres infractionnels tout à fait différents que représentent le web et les réseaux sociaux qui rendent obsolètes les moyens d'enquêtes classiques. En effet, lorsque, par exemple, un individu commet une infraction de pédopornographie sur un réseau social, les enquêteurs auront besoin de nouveaux moyens d'investigation pour obtenir des preuves. Il est crucial qu'ils puissent en disposer car, dans le cas contraire, l'Etat ne pourrait plus assurer son devoir de

[29] Fichier Automatisé des Empreintes Digitales qui, selon la CNIL sert à « sert à la recherche et à l'identification des auteurs de crimes et de délits ainsi qu'à l'identification de personnes condamnées à une peine privative de liberté ».

[30] Fichier National des Empreintes Génétiques, qui, selon la CNIL sert à « faciliter l'identification et la recherche des auteurs d'infractions à l'aide de leur profil génétique, et de personnes disparues à l'aide du profil génétique de leurs descendants ou de leurs ascendants ».

sécurité publique. La disproportion manifeste existant entre les moyens d'investigations et les infractions numériques aboutirait à des résultats inadéquats avec cette promesse.

C'est ce qu'affirme le ministère de l'Intérieur dans le projet de loi d'orientation et de programmation pour la performance de la sécurité intérieure dites LOPPSI 2 « Les délinquants utilisent de plus en plus les technologies modernes pour commettre des crimes et des délits ou pour dissimuler leurs agissements par des moyens techniques sophistiqués. Les forces de sécurité ne peuvent pas être à la traîne d'une délinquance de plus en plus violente ».

Deuxièmement, la nécessité pour les enquêteurs de se munir d'outils numériques modernes se rapporte à l'article L111-1 du CSI qui prévoit que « L'Etat a le devoir d'assurer la sécurité en veillant, sur l'ensemble du territoire de la République, à la défense des institutions et des intérêts nationaux, au respect des lois, au maintien de la paix et de l'ordre publics, à la protection des personnes et des biens ». La modification des techniques d'enquêtes par le biais des technologies numériques assure une rapidité et une efficacité dans la conduite des investigations qui leur a permis une amélioration concrète. En effet, les techniques de localisation GPS, vidéoprotection, d'exploitation du contenu d'un disque dur d'ordinateur ou du contenu d'un téléphone. La possibilité d'étendre les moyens d'enquêtes dans le cadre de certaines infractions (délinquance et criminalité organisée) et, si ce n'est l'enjeu le plus important, le troisième point concerne les cas les plus graves : le terrorisme.

Toutes ces possibilités désormais acquises ont permis une meilleure adaptation aux défis de la délinquance moderne. Cependant, ces acquis ne seront pas optimisés sur le long terme.

Le projet de loi d'orientation et de programmation du ministère de l'intérieur[31] prévoit de moderniser les moyens mis à la disposition des enquêteurs. Dans cet esprit, il affirme que « Le numérique, levier de modernisation et de rapprochement avec les citoyens à saisir mais aussi nouveau champ d'action à investir pour lutter notamment contre la cybercriminalité, impose au ministère de l'intérieur une « révolution copernicienne » comparable à la création de la police judiciaire sous Georges Clemenceau. Une part très importante des moyens de la présente loi est ainsi dédiée à la transformation numérique, pour que le ministère de l'intérieur se saisisse des opportunités qu'elle offre : démarches dématérialisées, outils de travail en mobilité, moyens d'investigation modernisés. Il est aussi un nouveau territoire de

[31] Projet de loi d'orientation et de programmation du ministère de l'intérieur n° 5185

délinquance de masse, qui demande à ce que des moyens humains, juridiques et budgétaires importants soient orientés vers la lutte contre la cybercriminalité, l'accompagnement des victimes et l'anticipation de la crise de demain »[32].

La conscience de l'importance cruciale d'intégrer les technologies numériques au sein des enquêtes n'est pas seulement trouvé sa place sur le plan National, mais aussi sur le plan européen. En effet, la compétitivité à l'échelle européenne et mondiale est l'un des enjeux majeurs de ces évolutions.

Lors de la pandémie de la Covid-19, les gouvernements mondiaux ont réfléchi à des façons de « surveiller » la propagation du virus au sein de la population. En renouant avec des moyens plus anciens tels que le confinement, la quarantaine, l'isolement ou encore la fermeture des frontières, la surveillance s'est démontrée sous de nouvelles formes : la reconnaissance faciale, les caméras et scanners thermiques, les applications de traçage, les drones. Ces nouveaux « agencements » de la surveillance continuent d'être expérimenté à tous les niveaux impliqués par la lutte contre la propagation du virus : l'échelle mondiale, nationale, régionale, locale et même individuelle[33].

Certains de ces moyens ont pu être évalués comme pertinents et ont été conservés alors que d'autres ont été jugés inacceptables, aggravant la panique sociale déjà présente par une panique morale. Des mouvements de protestations sont alors apparus pour s'opposer contre toute forme de contrôle social.

Dans cet ordre d'idées, certains citoyens qui ont très facilement accepté la présence des outils numériques dans la vie quotidienne, employant eux-mêmes nombreuses de ces technologies, n'autorisent pas de la même manière cet accès à l'Etat français. Ainsi, ils utilisent des innovations numériques telles que la reconnaissance faciale pour déverrouiller leurs téléphones portables[34] et tablettes ainsi que sur certaines applications dans le but d'appliquer des filtres sur le visage, le plus souvent sans savoir quel usage ces sociétés privées en feront.

En effet, les géants technologiques se sont approprié cette évolution, on peut penser au logiciel d'Apple « Iphoto » ou encore l'application « Picassa » et le réseau social Facebook

[32] Gérald DARMANIN, « Projet de loi nº 5185 d'orientation et de programmation du ministère de l'intérieur », 2022, https://www.assemblee-nationale.fr/dyn/15/textes/l15b5185_projet-loi#
[33] Les théories de la surveillance, Armand Colin
[34] Technologie disponible sur Android depuis 2011

qui utilisent ces logiciels de reconnaissance faciale. Le paradoxe de ce dernier vient du fait que ce sont les internautes eux-mêmes qui fournissent à ce réseau des millions de photographies par jour. Ajoutons à cela que quotidiennement une centaine de millions de noms sont légendés sous ces visages partagés au quotidien. Dès lors, cela permet au réseau social de récolter de nombreuses informations sur ses utilisateurs. Ces dernières sont leurs données personnelles sur lesquelles il base son système économique.

Mais les exemples ne s'arrêtent pas là, les appareils tels que les smartphones modernes ou les enceintes connectées utilisent la reconnaissance vocale pour permettre à son utilisateur d'effectuer des commandes vocales en collectant des données sur la voix des individus. Pour fonctionner, ces logiciels doivent constamment être activés c'est-à-dire que tout au long de la journée et même la nuit, le téléphone écoutera et traitera les conversations qu'il captera.

A ce titre, il faut ajouter qu'il a pris une place primordiale dans notre vie quotidienne et, de ce fait, se trouve la plupart du temps à portée de voix. De même que pour la reconnaissance faciale, la plupart des utilisateurs n'ont pas conscience de la portée de leur consentement aux conditions d'utilisations. Une troisième technologie est utilisée par ces appareils mais aussi désormais par les tablettes et certains ordinateurs : les empreintes digitales. Elles sont utilisées non seulement pour déverrouiller mais aussi pour valider un paiement bancaire ou accéder à une application particulière par exemple.

Concrètement, ce sont des appareils technologiques qui enregistrent les données biométriques des individus. Plus spécifiquement, la CNIL définit la biométrie comme regroupant « l'ensemble des techniques informatiques permettant de reconnaître automatiquement un individu à partir de ses caractéristiques physiques, biologiques, voire comportementales »[35]. Elle ajoute que ce sont des données personnelles puisqu'elles permettent d'identifier une personne. Pour la plupart, elles ont pour particularité d'être uniques et permanentes comme par exemple l'ADN ou les empreintes digitales.

De plus, la biométrie signifie littéralement « la mesure du corps humain ». C'est pour cette raison qu'il existe deux catégories de technologies biométriques, tout d'abord les mesures physiologiques qui peuvent être morphologiques ou biologiques. Les premières regroupent principalement l'œil (iris et rétine), les empreintes digitales, la forme du doigt et de la main

[35] CNIL, « Biométrie », https://www.cnil.fr/fr/definition/biometrie

mais aussi du visage. Les secondes comprennent l'ADN, la salive, le sang ou l'urine qui peuvent être utilisées dans le domaine médical et des investigations par exemple[36].

Les mesures comportementales quant à elles sont caractérisées par la reconnaissance vocale, la démarche mais aussi la dynamique des signatures, telles que l'inclinaison du stylet, sa vitesse de déplacement, et celle de frappe du clavier d'un ordinateur.

Pour en revenir au raisonnement initial, certains des utilisateurs qui accordent aux sociétés privées d'avoir un large accès à leur données personnelles, ont une toute autre appréhension des enjeux lorsqu'il est question d'accorder leur consentement à l'Etat. En effet, les citoyens sont, pour la plupart, réticents à l'idée de laisser ce dernier disposer de leurs données biométriques, se justifiant par l'atteinte aux droits et libertés individuelles qui en découlerait.

Bien que l'objectif du législateur soit de récolter et traiter ces données personnelles pour assurer la sécurité publique, dans une conscience collective, pour certains individus cela représente un risque trop important de voir l'apparition d'une société de surveillance à l'image de la célèbre prophétie littéraire de George Orwell « Big brother is watching you »[37]. La possibilité que les dirigeants utilisent ces nouvelles technologies aux fins de contrôler la population apparaît comme trop effrayante pour menacer les libertés individuelles, fusse-t-elle choisie au détriment de la sécurité.

A ce sujet, les avis sont partagés puisqu'une autre partie des citoyens considère qu'il est naturel de céder quelques libertés individuelles si l'objectif est d'assurer une sécurité publique collective dont tout un chacun en bénéficiera. Cette double vision conduit l'Etat à faire face à une problématique importante : la conciliation des technologies de sécurité avec les libertés. En définitive, il s'agit pour lui de moderniser notre arsenal juridique en poursuivant l'objectif de prévention des atteintes à l'ordre public sans sacrifier les autres exigences constitutionnelles.

Toutes ces mesures n'ont cependant pas le même degré de fiabilité, alors que l'ADN permet d'établir avec certitude certains faits lors d'une enquête, la reconnaissance faciale est une étude qui est loin d'être aussi fiable. C'est aussi le cas plus récemment des technologies

[36] Thales, « La biométrie au service de l'identification et l'authentification », 2021, https://www.thalesgroup.com/fr/europe/france/dis/gouvernement/inspiration/biometrie

[37] George Orwell, *1984*, Secker and Warburg, 8 juin 1949

avancées telles que les logiciels d'intelligence artificielle de prédiction des crimes dont les progrès scientifiques ne permettent pas d'assurer un fonctionnement sans faille[38].

Cependant les avancées technologiques ont d'ores et déjà prouvé leur efficacité. C'est le cas de l'identification de Mohamed Abrini, « l'homme au chapeau » des attentats de Bruxelles, qui a été rendue possible grâce à un logiciel de reconnaissance faciale développé par le Federal Bureau of Investigation.

En définitive, si la nécessité d'adaptation des moyens d'enquêtes aux outils numériques n'est plus à établir, la conformité de ces évolutions aux droits et libertés fondamentaux doit cependant être examinée de près par le Conseil constitutionnel. Le garant de ces droits et libertés représente en effet un bouclier face aux atteintes potentielles mais aussi une balance permettant de trouver un équilibre proportionné entre le devoir de sécurité publique et celui de protection des droits et libertés.

§2 Les évolutions juridiques subséquentes

« Nul ne peut agir avec l'intensité que suppose l'action criminelle sans laisser des marques multiples de son passage »[39].

Avant l'essor des technologies numériques, les marques laissées par un délinquant sur une scène d'infraction étaient exclusivement humaines et matérielles. En effet, les objets peuvent laisser des traces (arme à feu, semelles de chaussures) qui n'identifient pas directement leur utilisateur. Les humains quant à eux, sont à l'origine de traces papillaires dont « le dessin papillaire présent sur ces différentes zones étant permanent et unique, il est donc possible, à partir d'une trace papillaire, d'identifier son auteur. »[40]

[38] Ces affirmations seront détaillées au sein du §1, section 2 de ce même chapitre

[39] Edmond LOCARD

[40] Pôle Judiciaire de la Gendarmerie Nationale, « Les traces papillaires ensanglantées », https://www.gendarmerie.interieur.gouv.fr/pjgn/ircgn/l-expertise-decodee/identification/les-traces-papillaires-ensanglantees

Depuis lors, les délinquants sont aussi à l'origine de traces immatérielles qui résultent de l'emploi d'outils technologiques comme l'utilisation d'un téléphone portable, du GPS ou encore de sa carte bancaire. C'est sur ces données que se portent, aujourd'hui, systématiquement les analyses des enquêteurs : l'exploitation des supports numériques mais aussi les images prises à partir des appareils de vidéoprotection et les données provenant des téléphones portables[41].

A) Le développement des techniques modernes d'enquêtes

Les outils numériques plus sophistiqués, en raison de leurs atteintes aux libertés individuelles, ne peuvent être employés que dans certaines conditions préalablement prévues. La loi n°2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice a permis de regrouper certaines investigations au sein de la section 6 du chapitre II (Titre XXV du Livre IV) du code de procédure pénale intitulé « Des autres techniques spéciales d'enquêtes ». Ce chapitre concerne trois catégories de mesures telles que l'IMSI catcher, la sonorisation et fixation d'images de certains lieux et véhicules et la captation de données informatiques. Quant au terme « autres », il suggère un lien avec les techniques applicables en matière de criminalité et délinquance organisée mais aussi par leur nature très intrusive qu'elles ont en commun avec les mécanismes semblables d'interception. Ces techniques spéciales existaient déjà avant la loi et reposaient sur des dispositions communes c'est pourquoi le législateur les a regroupées.

Le premier dispositif numérique en cause permet le recueil des données techniques de connexion et l'interception de correspondances émises par la voie des communications électroniques. Appelé IMSI catcher il est utilisé, selon l'article 706-95-20 I du CPP « afin de recueillir les données techniques de connexion permettant l'identification d'un équipement terminal ou du numéro d'abonnement de son utilisateur, ainsi que les données relatives à la localisation d'un équipement terminal utilisé ». Les termes de cet article permettent ainsi de retenir l'usage possible de ce dispositif de proximité dans le but de capter des données

[41] Marc Schwendenert, « Police technique et scientifique », *Répertoire de droit pénal et de procédure pénale*, 2016, https://www-dalloz-fr.lama.univ-amu.fr/documentation/Document?ctxt=0_YSR0MD1Qb2xpY2UgdGVjaG5pcXVlIGV0IHNjaWVudGlmaXF1ZSDCp3gkc2Y9c2ltcGxlLXNlYXJjaA%3D%3D&ctxtl=0_cyRwYWdlTnVtPTHCp3MkdHJpZGF0ZT1GYWxzZcKncyRzb3J0PSNkZWZhdWx0X0Rlc2PCp3Mkc2xOYlBhZz0yMMKncyRpc2Fibz1UcnVlwqdzJHBhZ2luZz1UcnVlwqdzJG9uZ2xldD3Cp3MkZnJlZXNjb3BlPUZhbHNlwqdzJHdvSVM9RmFsc2XCp3Mkd29TUENIPUZhbHNlwqdzJGZsb3dNb2RlPUZhbHNlwqdzJGJxPcKncyRzZWFyY2hMYWJlbD3Cp3Mkc2VhcmNoQ2xhc3M9&id=ENCY%2FPEN%2FRUB000387

techniques de connexion utiles « à une enquête ou information judiciaire intéressant la criminalité et la délinquance organisées, spécialement sur le terrain terroriste »[42]. Cependant, seuls sont concernés les éléments d'identification des appareils ciblés et non le contenu des correspondances.

Mais il est aussi possible d'employer ce dispositif dans le but d'intercepter des correspondances émises par la voie des communications électroniques. C'est le II du même article qui le prévoit : « Il peut être recouru à la mise en place ou à l'utilisation de cet appareil ou de ce dispositif afin d'intercepter des correspondances émises ou reçues par un équipement terminal ». L'utilisation de cet outil numérique était initialement prévue comme un moyen de police administrative puis a été étendu au domaine judiciaire depuis la loi du 24 juillet 2015 relative au renseignement[43].

Ensuite, un dispositif de sonorisation et fixation d'images a été étendu à l'enquête pour des raisons d'efficacité répressive. En effet, l'article 706-96 CPP prévoit que « Il peut être recouru à la mise en place d'un dispositif technique ayant pour objet, sans le consentement des intéressés, la captation, la fixation, la transmission et l'enregistrement de paroles prononcées par une ou plusieurs personnes à titre privé ou confidentiel, dans des lieux ou véhicules privés ou publics, ou de l'image d'une ou de plusieurs personnes se trouvant dans un lieu privé ».

Enfin, peut désormais être utilisé un dispositif de captation des données informatiques aussi bien lors d'enquêtes préliminaires que de flagrance. C'est l'article 706-102-1 alinéa 1 CPP qui prévoit son utilisation : « Il peut être recouru à la mise en place d'un dispositif technique ayant pour objet, sans le consentement des intéressés, d'accéder, en tous lieux, à des données informatiques, de les enregistrer, de les conserver et de les transmettre, telles qu'elles sont stockées dans un système informatique, telles qu'elles s'affichent sur un écran pour l'utilisateur d'un système de traitement automatisé de données, telles qu'il les y introduit par saisie de caractères ou telles qu'elles sont reçues et émises par des périphériques ».

---

[42] Yves Mayaud, « Terrorisme – Poursuites et indemnisation », *Répertoire de droit pénal et de procédure pénale*, 2020, https://www-dalloz-fr.lama.univ-amu.fr/documentation/Document?id=ENCY%2FPEN%2FRUB000396%2F2020-02%2FPARA%2F272&ctxt=0_YSR0MD10ZWNobmlxdWVzIHNww6ljaWFsZXMgZCdlbnF1w6p0ZcKneCRzZj1zaW1wbGUtc2VhcmNo&ctxtl=0_cyRwYWdlTnVtPTHCp3MkdHJpZGF0ZT1GYWxzZcKncyRzb3J0PSNkZWZhdWx0X0Rlc2PCp3Mkc2xOYlBhZz0yMMKncyRpc2Fibz1UcnVlwqdzJHBhZ2luZz1UcnVlwqdzJG9uZ2xldD3Cp3MkZnJlZXNjb3BlPUZhbHNlwqdzJHdvSVM9RmFsc2XCp3Mkd29TUENIPUZhbHNlwqdzJGZsb3dNb2RlPUZhbHNlwqdzJGJxPcKncyRzZWFyY2hMYWJlbD3Cp3Mkc2VhcmNoQ2xhc3M9&scrll=ENCY%2FPEN%2FRUB000396%2F2020-02%2FPARA%2F273

[43] Loi n°2015-912 du 24 juillet 2015 relative au renseignement

De cette manière, il est désormais possible pour les enquêteurs d'appliquer des méthodes modernes d'enquête, intégrant les dernières avancées technologiques. Ces techniques spéciales permettent aux enquêteurs de recueillir des informations sans alerter les personnes suspectes. Ainsi, non seulement ces outils numériques permettent à ces derniers d'agir de façon plus efficace dans leurs recherches mais également de le faire en toute discrétion. En revanche, elles ne sont prévues que pour les infractions précitées[44].

Reconnaissance faciale. Une autre technologie avancée est aujourd'hui essentiellement utilisée à titre expérimental en France : la reconnaissance faciale. La Commission Nationale de l'Informatique et des Libertés (CNIL), régulateur des données personnelles, définit la reconnaissance faciale comme « une technique qui permet à partir des traits de visage d'authentifier une personne : c'est-à-dire, vérifier qu'une personne est bien celle qu'elle prétend être (dans le cadre d'un contrôle d'accès) ou d'identifier une personne : c'est-à-dire, de retrouver une personne au sein d'un groupe d'individus, dans un lieu, une image ou une base de données. »

Ce procédé, réalisé à partir d'une image fixe, comme une photo, ou animées, comme un enregistrement vidéo, se construit en plusieurs phases : l'image préalablement récoltée va servir de « modèle » pour réaliser les caractéristiques de ce visage.

Ces données récoltées sont appelées données « biométriques » et sont définies par le RGPD, dans son article 4-14, comme « les données à caractère personnel résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique, qui permettent ou confirment son identification unique, telles que des images faciales ou des données dactyloscopiques »

La seconde phase est celle de la « reconnaissance » qui est réalisée en comparant les modèles stockés avec les modèles calculés directement sur les visages présents au sein de la vidéo ou de l'image que l'on souhaite contrôler.

La reconnaissance faciale se base sur plusieurs caractéristiques du visage pour différencier 2 images efficacement et obtenir le score de similarité le plus important parmi les visages qui dépassent un seuil prédéterminé. Ce sont l'espacement entre les yeux, la base des oreilles,

[44] Criminalité et délinquance organisée

les contours de la bouche, du nez qui vont permettre de reconstruire la forme 3D du visage de l'individu.

Plusieurs expérimentations ont été menées en France notamment à la gare du nord à Paris en 2017 pour passer les douanes lorsque l'on prend Eurostar, la société Aéroports de Paris depuis 2018. Ce fut également le cas lors du carnaval de Nice en 2019 et du tournoi de Roland-Garros en 2020 pour tester un dispositif de contrôle d'accès pour les arbitres. En France, il est aussi utilisé par les services d'enquêteurs pour retrouver des enfants disparus à partir de sites pédopornographiques.

Dispositifs aéroportés. La loi du 24 janvier 2022[45] relative à la responsabilité pénale et à la sécurité intérieure a inséré dans le code de la sécurité intérieure les articles L. 242-1 à L. 242-8 au sein du chapitre II du titre IV du livre II qui déterminent le régime juridique des caméras aéroportées en matière de police administrative. Ce régime juridique comporte dorénavant des garanties plus protectrices du droit au respect de la vie privée qu'au sein de la loi « sécurité globale ».

L'article L242-5 prévoit que « Dans l'exercice de leurs missions de prévention des atteintes à l'ordre public et de protection de la sécurité des personnes et des biens, les services de la police nationale et de la gendarmerie nationale ainsi que les militaires des armées déployés sur le territoire national dans le cadre des réquisitions prévues à l'article L. 1321-1 du code de la défense peuvent être autorisés à procéder à la captation, à l'enregistrement et à la transmission d'images au moyen de caméras installées sur des aéronefs ».

Les drones permettent de faciliter la recherche de personnes, l'identification de suspects mais aussi de procéder à des constatations sur le lieu de commission d'une infraction ou faciliter le recueil d'éléments de preuves. Ils sont discrets et mobiles, peuvent se déplacer dans le ciel sans être aperçus, suivre une personne, filmer une foule voir même filmer l'intérieur d'un domicile par la fenêtre selon certaines situations. De cette manière, ils constituent un atout d'une grande importance puisqu'ils permettent aux policiers de déplacer aisément la caméra et de voir en temps réel les images captées par l'appareil.

En revanche, il n'est pas encore possible de combiner l'usage d'un drone avec un dispositif de reconnaissance faciale. La loi Responsabilité pénale et sécurité intérieure prévoit ainsi

[45] Loi n° 2022-52 du 24 janvier 2022 relative à la responsabilité pénale et à la sécurité intérieure

que les drones ne pourront pas « comporter de traitements automatisés de reconnaissance faciale ».

B) La création de logiciels à la disposition des enquêteurs

Les services d'enquêtes disposent aussi de logiciels de rapprochement et d'analyse judiciaires notamment le logiciel Anacrim, un outil d'aide à l'enquête, qui fut créé par la loi du 14 mars 2011[46]. Cette loi a inséré les articles 230-20 à 230-27 du code de procédure pénale dont le premier dispose que « *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 logiciels destinés à faciliter l'exploitation et le rapprochement d'informations sur les modes opératoires réunies par ces services au cours : 1° Des enquêtes préliminaires, des enquêtes de flagrance ou des investigations exécutées sur commission rogatoire ; 2° Des procédures de recherche des causes de la mort ou d'une disparition prévues par les articles 74 et 74-1.* »

Utilisé à la fois par le service central de renseignements criminels de la gendarmerie nationale (SCRC), par l'Office central de la répression de la violence aux personnes (OCRVP) de la police nationale[47], cet outil technologique permet de croiser tous les indices recueillis sur une affaire. Mis en œuvre depuis 1994, ce logiciel rassemble plusieurs « logiciels de rapprochement judiciaire à des fins d'analyse criminelle » selon la Cnil. Plus précisément, il permet sur une base de données conséquentes relative à une affaire, grâce à sa capacité de traitement hors normes, de mettre en avant toutes les anomalies que l'humain n'aurait pas pu déceler. Ainsi, les enquêteurs peuvent découvrir des contradictions de témoignage, des informations incohérentes qui seront susceptibles, à terme, de résoudre l'affaire. C'est ce logiciel qui a notamment permis de compléter l'enquête dite du « petit Grégory » plus de 30 ans après les faits alors que la police ne parvenait pas à la résoudre.

[46] Loi n°2011-267

[47] Philippe Rioux, « Les nouvelles techniques d'enquête », 2017, https://www.ladepeche.fr/article/2017/06/17/2595775-les-nouvelles-techniques-d-enquete.html

D’autres logiciels ont été mis à la disposition des enquêteurs dans le but notamment de centraliser les données conservées sur les données biométriques des individus. Le FAED et le FNAEG, deux fichiers à la disposition des enquêteurs judiciaires que nous avons évoqués plus tôt, permettent d’identifier et d’authentifier des personnes à partir de l’enregistrement d’empreintes papillaires et génétiques de certains individus.

Concernant tout d’abord le FAED, il est employé pour « la recherche et à l’identification des auteurs de crimes et de délits ainsi qu’à l’identification de personnes condamnées à une peine privative de liberté. Il permet par ailleurs de faciliter la recherche de personnes disparues ou l’identification de personnes décédées ou grièvement blessées. Il est également utilisé pour vérifier l’identité de personnes retenues en application de l’article 78-3 du code de procédure pénale ou dans les conditions prévues par l’article L. 611-4 du code de l’entrée et du séjour des étrangers et du droit d’asile »[48].

Quant au FNAEG, il permet de « faciliter l’identification et la recherche des auteurs d’infractions à l’aide de leur profil génétique, et de personnes disparues à l’aide du profil génétique de leurs descendants ou de leurs ascendants »[49]. L'enregistrement des empreintes ou traces se réalise dans le cadre d'une enquête pour crime ou délit, d'une enquête préliminaire, d'une commission rogatoire ou de l'exécution d'un ordre de recherche délivré par une autorité judiciaire d’après l’autorité de contrôle.

Les données de ces deux fichiers automatisés peuvent être conservées entre 20 et 40 ans selon la qualité de la personne : personnes définitivement condamnées, décédées, les personnes disparues, mises en cause etc…

Enfin, un dernier fichier nommé le Traitement des Antécédents Judiciaires (TAJ) est un fichier commun à la police et à la gendarmerie nationale qui, « en application des articles 230-6 à 230-11 du Code de procédure pénale, est utilisé dans le cadre des enquêtes judiciaires (recherche des auteurs d’infractions) et d’enquêtes administratives (comme les enquêtes préalables à certains emplois publics ou sensibles) »[50]. Il contient des informations sur les personnes mises en cause et sur les victimes.

[48] CNIL, « FAED : Fichier automatisé des empreintes digitales », 2018, https://www.cnil.fr/fr/faed-fichier-automatise-des-empreintes-digitales

[49] CNIL, « FNAEG : Fichier national des empreintes génétiques », 2018, https://www.cnil.fr/fr/fnaeg-fichier-national-des-empreintes-genetiques

[50] CNIL, « TAJ : Traitement d’Antécédents Judiciaires », 2018, https://www.cnil.fr/fr/taj-traitement-dantecedents-judiciaires

Logiciel de centralisation des informations. Afin de simplifier et de rendre plus efficace le travail des enquêteurs, plusieurs techniques d'enquêtes numériques judiciaires ont été mises à leur disposition. Les enquêteurs ont ainsi accès à des logiciels créés et adaptés à l'évolution des technologies numériques mais sont aussi habilités à réaliser des réquisitions informatiques, demander la mise au clair des données cryptées lorsqu'elle est nécessaire à la manifestation de la vérité, effectuer des saisies, de la géolocalisation et même des enquêtes sous pseudonyme ou infiltration.

La plateforme Nationale des Interceptions judiciaires (PNIJ) est une plateforme de traitement automatisé de données à caractère personnel placée sous la responsabilité du secrétaire général du ministère de la justice[51]. Régie par les articles R. 40-42 à R. 40-56 du code de procédure pénale, cet organisme « centralise l'ensemble des réquisitions judiciaires adressées aux opérateurs de communications électroniques et met les données reçues en réponse à la disposition des magistrats et des agents habilités des services de police, de gendarmerie, de la douane judiciaire et des services fiscaux »[52].

De cette manière, la plateforme a permis de centraliser les interceptions judiciaires. En effet, auparavant, le système en place nécessitait le recours à des sociétés privées ainsi qu'à la location de moyens d'enregistrement et d'écoute. Désormais, les enquêteurs judiciaires peuvent intercepter tout type de communication directement depuis la PNIJ. Cela leur permet d'avoir accès aux conversations orales, aux SMS, MMS, que ces derniers soient stockés sur un ordinateur, une tablette ou encore un téléphone portable.

De surplus, avant sa mise en place, seule l'Officier de Police Judiciaire (OPJ) saisi sur commission rogatoire technique avait la qualification pour accéder aux interceptions judiciaires en cours. Ensuite, il retranscrivait les communications qui lui paraissaient utiles à la manifestation de la vérité. Aujourd'hui, les magistrats ont directement accès à ces communications à partir de la plateforme et peuvent les consulter sans passer par l'OPJ. C'est un apport important qui concerne la gestion des scellés. En effet, il n'est plus nécessaire de placer les interceptions sur un CD Rom sous scellé fermé et de l'exploiter par la transmission des enquêteurs d'une copie de leur travail ou en passant par une procédure de bris de scellés en présence du mis en examen ou son avocat.

---

[51] Constance Le Grip, 15ème législature Question N° 3287, 2017-2018, https://questions.assemblee-nationale.fr/q15/15-3287QE.htm

[52] Article R40-42 CPP

Plate-forme nationale des interceptions judiciaires. Dans le cadre d'une enquête judiciaire, les enquêteurs et les magistrats en charge du dossier sont amenés à collecter des informations, par l'emploi de plusieurs dispositifs comme la géolocalisation, la collecte de données de connexion, la pose de micro, l'interception des conversations, etc.

Dans un objectif de centralisation des données, l'Agence Nationale des Techniques d'Enquêtes Numériques Judicaires (ANTENJ) met en œuvre un traitement de données, prénommé Plate-forme nationale des interceptions judiciaires (PNIJ). L'ANTENJ est un service à compétence nationale qui relève du garde des sceaux[53].

Cette plateforme permet de mettre à disposition ces données, de manière sécurisée, uniquement aux utilisateurs habilités dans le cadre de l'exercice de leurs fonctions judiciaires (enquêteurs, magistrats, ...)[54].

Section 2) Les défis engendrés par l'évolution rapide des technologies numériques

L'intégration de technologies numériques au sein des enquêtes a entraîné l'apparition des défis à la fois humains, par l'adaptation des enquêteurs à leur usage (§1), mais aussi de failles techniques dans l'application de certains outils numériques à des situations réelles (§2).

§1 Les défis humains d'adaptation des enquêteurs à ces technologies

La sophistication des objets connectés (smartphone, ordinateur portables…) permet aux enquêteurs de recueillir des informations dont le nombre et la précision augmente de plus en plus en raison de la polyvalence croissante de ces appareils : cellules activées, traces ou historiques de connexions internet, géolocalisation, facturations détaillées (« fadettes »), utilisation de certains logiciels de messagerie, etc…

[53] Ministère de la Justice, « Informatique et libertés : Plate-forme nationale des interceptions judiciaires », 2022, https://www.justice.fr/donnees-personnelles/PNIJ
[54] Idem

Les enquêteurs rencontrent, par ce biais, des complications liées à la complexité d'analyse des smartphones et au cryptage dont ils font l'objet. En effet, non seulement le nombre d'informations stockées à l'intérieur et leur diversification croît de façon importante mais, de surplus, leur exploitation est de plus en plus ardue.

Selon Marc Schwendener, commissaire divisionnaire de police de la police nationale, « le bras de fer auquel se livrent les autorités judiciaires de certains pays et les fabricants de smartphones et d'outils de cryptage pour permettre aux premières d'accéder aux données échangées ou stockées par ces biais atteste de l'importance de cet enjeu ».

Les progrès effectués dans le domaine des enquêtes judiciaires engendrées par le développement du numérique sont donc à l'origine de difficultés pour les enquêteurs.

Tout d'abord, il faut relever un point important : la formation. Le premier obstacle que rencontrent les services d'enquêtes se trouve au stade de la formation des agents. En effet, les possibilités de collecte des preuves matérielles dans les affaires judiciaires ont considérablement augmenté ces dernières années. Les preuves numériques peuvent désormais être récoltées à partir de téléphones portables, ordinateurs, disques durs et bien sûr à partir d'Internet plus généralement. Ainsi, il est nécessaire que les forces de police comptent parmi leurs effectifs des spécialistes qui soient capables d'exploiter et d'interpréter ces données.

Subséquemment, c'est leur formation qui nécessite d'être mise à jour. En effet, alors que les appareils numériques modernes sont fabriqués à partir de technologies de plus en plus abouties et complexes, les compétences des agents ne sont pas mises à niveau. Malgré l'apparition de postes spécialisés dans la cybersécurité, ils sont encore trop peu nombreux. Prenons l'exemple du commissariat de police d'Avignon[55], au sein du pôle « sécurité publique », il n'existe qu'un seul spécialiste, alors même qu'il contient de très nombreux agents de police. Ainsi, il sera sollicité dans toutes les affaires qui nécessitent l'exploitation d'un appareil technologique, ce qui représente une charge de travail très importante pour une seule et unique personne. Une formation plus approfondie dans ce domaine devrait être fournie à tous les enquêteurs dans leur formation initiale. Même si le budget qui devra y être alloué est important, le bénéfice retiré dans la conduite des investigations en termes de gain de temps et d'efficacité le sera bien plus.

[55] Cette constatation a été faite lors de mon stage au sein du commissariat de Police d'Avignon.

Les données massives. La deuxième difficulté inextricablement liée à la première concerne la quantité de données que les enquêteurs ont pour mission de traiter. Des données numériques sont désormais produites dans chacune de nos actions effectuées à partir d'un outil numérique au travail ou à titre privé. Pour obtenir un ordre d'idée, le volume de données numériques créées ou répliquées à l'échelle mondiale se compte aujourd'hui en zettaoctets[56]. Alors que la quantité de données produites en 1 an était de 2 zettaoctets en 2010, elle a été multipliée par 32 entre 2010 et 2020 pour atteindre 64,2 zettaoctets.

En conséquent, même si les effectifs d'enquêteurs sont indubitablement insuffisants, leur augmentation ne permettra pas de résoudre cette difficulté sur le long terme. C'est pourquoi l'emploi de technologies numériques capables de traiter ces données quantitativement impressionnantes est d'ores et déjà une solution à envisager.

Il est aussi primordial de renforcer les effectifs de police. Le renseignement numérique mais aussi l'écoute des flux de données de téléphone, permet aux forces de police d'avoir accès à des contenus auparavant inaccessibles. Les flux d'images, de vidéos, les messages échangés sur les applications WhatsApp, Skype et Messenger, mais également les métadonnées, les données de service de téléphone comme la localisation, les horaires d'utilisation sont autant de nouvelles ressources à exploiter pour les services techniques.

Ces nouveaux outils permettent aux forces de sécurité d'agrandir l'arsenal des sources d'informations à consulter dans le cadre de leur mission. Par conséquent, alors que la quantité de données à traiter augmente sans cesse, les effectifs de police quant à eux ne se multiplient pas, ce qui engendre nécessairement une surcharge de travail qui peut être préjudiciable pour l'enquête. A quoi servirait l'opportunité d'accéder à un si grand nombre de données pour la conduite des investigations si elles ne peuvent pas être exploitées ?

[56] 1 zettaoctet correspond mille milliards de milliards d'octets

§2 L'apparition de failles numériques dans les outils de lutte contre la délinquance

A) L'existence de biais cognitifs

« Il faut éviter que les biais de la société ne se reflètent dans les décisions prises par les machines » a affirmé Yann LeCun, chercheur en intelligence artificielle et vision artificielle.

Tout d'abord, *qu'est-ce qu'un biais* ? En vieux provençal, le terme « biais » signifie tournant ou détour. Un biais cognitif peut être entendu comme « tendances et inclinations systémiques de notre esprit, que nous jugeons souvent irrationnelles »[57].

L'Intelligence Artificielle est un outil créé par l'Homme et, de cette manière, peut reproduire les préjugés des développeurs. C'est alors que des biais cognitifs pourront être engendrés. La manière dont le programme ou l'algorithme sera rédigés déterminera les forces et les faiblesses du système. En outre, au sein des mécanismes d'Intelligence Artificielle différents types de biais peuvent être rencontrés.

Prenons l'exemple d'un logiciel de reconnaissance faciale, c'est une intelligence artificielle qui s'appuie sur l'apprentissage statistique qui détermine ses choix selon des probabilités. De cette manière, il est impossible d'identifier quel paramètre aura été déterminant dans la décision lorsque l'on sait que chaque paramètre créé peut avoir une incidence sur un autre. Une problématique apparaît alors : cet outil numérique fonctionne à l'aide d'algorithmes qui retranscrivent les biais humains. En d'autres termes, si on intègre des biais raciaux au sein du système, il va automatiquement les recréer lorsqu'il effectuera un choix. De la même manière, si l'algorithme est réalisé à partir du profil d'hommes blancs, l'appareil fonctionnera moins bien si les sujets sont des femmes ou des personnes de couleur.

Ainsi, les programmeurs des logiciels numériques utilisant l'Intelligence artificielle par apprentissage statistiques pourront transmettre leurs biais dits « cognitifs » à leur création

[57] Gérard HAAS, Stéphane ASTIER, « Les biais de l'intelligence artificielle : quels enjeux juridiques ? » *Répertoire IP/IT et Communication*, 2019, https://www-dalloz-fr.lama.univ-amu.fr/documentation/Document?id=ENCY%2FIPIT%2FRUB000429&ctxt=0_YSR0MD1Hw6lyYXJkIEhBQVMsIFN0w6lwaGFuZSBBU1RJRVIgTGVzIGJpYWlzIGRlIGwnaW50ZWxsaWdlbmNlIGFydGlmaWNpZWxsZSA6IHF1ZWxzIGVuamV1eCBqdXJpZGlxdWVzIMKneCRzZj1zaW1wbGUtc2VhcmNo&ctxtl=0_cyRwYWdlTnVtPTHCp3MkdHJpZGF0ZT1GYWxzZcKncyRzb3J0PSNkZWZhdWx0X0Rlc2PCp3Mkc2xOYlBhZz0yMMKncyRpc2Fibz1UcnVlwqdzJHBhZ2luZz1UcnVlwqdzJG9uZ2xldD3Cp3MkZnJlZXNjb3BlPUZhbHNlwqdzJHdvSVM9RmFsc2XCp3Mkd29TUENIPUZhbHNlwqdzJGZsb3dNb2RlPUZhbHNlwqdzJGJxPcKncyRzZWFyY2hMYWJlbD3Cp3Mkc2VhcmNoQ2xhc3M9&scrll=ENCY%2FIPIT%2FRUB000429%2F2019-09%2FSOMMAIRE

s’ils en possèdent initialement. La raison principale est qu’ils sont liés à la manière dont les algorithmes sont rédigés par les programmeurs. Ils représentent une forme de distorsion de la manière dont l'information sera traitée par rapport à la réalité ou à un comportement rationnel.

De ce fait, sont particulièrement concernés les systèmes d’apprentissage statistiques appelés Machine Learning qui se définit comme « une science moderne permettant de découvrir des répétitions (des patterns) dans un ou plusieurs flux de données et d’en tirer des prédictions en se basant sur des statistiques ». En d’autres termes, cela signifie que les ordinateurs, à partir d’une base de données (le Big Data), sont capables d’apprendre sans avoir été programmés à cela. Ainsi, ils pourront prédire une action future à partir d’un ensemble d’éléments répétitifs passés en calculant les probabilités que cela se produise.

Pour ce faire, cette technologie effectuera ses choix selon telle ou telle probabilité : « il existe 80% de chances que cette photo représente un chien » par exemple. D’après David Sadek, vice-président de recherche, technologie et innovation chez Tales, « Ce sont des boîtes noires. On ne sait pas pourquoi la machine aboutit à tel ou tel résultat, même si on connaît les mathématiques qu'elle a utilisées. »

Il continue son explication en disant que « Même si on arrive à isoler le paramètre déterminant, dire 'le copilote virtuel d'un avion conseille de virer de 30° parce que la valeur du paramètre 3695 est 3', ça peut ne rien signifier pour le pilote. En revanche, il conseille cela parce qu'il détecte un orage droit devant, c'est compréhensible. »

Il existe d’autres cas, pour lesquels, le concepteur va favoriser une vision du monde alors même que les données disponibles vont remettre en question cette vision. On appelle cela les « biais d’anticipation » ou de « confirmation ». Dans certains cas, le développeur peut avoir adopté une ou plusieurs modélisations populaires sans pour autant s'assurer de leur exactitude. On parle alors de biais dits de Bandwagon ou bien « du mouton de Panurge ». Une autre hypothèse ne met pas en cause l’intervention consciente du programmeur dans le biais, c’est le rapprochement de deux éléments qui sont indépendants et qui produisent ce qu’on appelle les « biais de corrélation illusoire »[58].

Ces différents types de biais algorithmiques proviennent cependant tous de l’action du concepteur qu’elle ait été consciente ou inconsciente. C’est d’ailleurs ce qu’affirme la loi de

[58] Idem

Kranzberg : « la technologie n'est ni mauvaise, ni bonne, ni neutre, elle est ce qu'on en fait ».

Les conséquences qui découleraient de l'existence de tels biais ne sont pas à prendre à la légère. Le développement par deux chercheurs américains de l'IA qui, à partir de l'analyse de 35 000 photographies avait pour commande d'identifier l'orientation sexuelle des individus à partir de leur visage en est l'illustration flagrante[59]. Le simple objet de cette recherche est totalement déplacé. L'introduction de biais cognitifs dans ce projet, seulement au stade du choix, par les chercheurs laisse présager l'importance des déviances des résultats ainsi que les risques d'une exploitation à grande échelle.

Une illustration des conséquences négatives résultant de ces biais a été observée aux Etats-Unis. En janvier 2020, un Afro-Américain a été arrêté dans le Michigan pour un vol à l'étalage. Il a été arrêté et mis en détention par les policiers en se basant sur le résultat d'une Intelligence artificielle de reconnaissance faciale. Celle-ci n'avait cependant pas appris à différencier les visages noirs parce que ses entraînements avaient été effectués sur des images représentant essentiellement des visages blancs. Rapidement, le visage de l'homme avait été comparé aux vidéos de surveillance du magasin en question et, n'ayant aucune ressemblance avec le délinquant, il a rapidement été relâché.

En 2016, l'ONG pro-publica annonçait que le logiciel de Justice prédictive COMPAS contenait des biais à l'encontre des populations afro-américaines. Cet algorithme prédictif permet de déterminer les risques de récidive d'un criminel. Utilisé par de nombreux tribunaux Américains, son objectif était d'aider le magistrat à prendre des décisions d'incarcération en se basant sur le risque de récidive des délinquants condamnés obtenu à partir du logiciel. Ce dernier recueil des informations sur l'individu qui concernent son emploi, sa famille, ses habitudes de vie notamment. La polémique a totalement remis en cause ce dispositif. Tous ces exemples démontrent un fort besoin de régulation.

L'expérience « Moral Machine ». En 2014, des chercheurs du MIT Media Lab ont créé une expérience intitulée « Moral Machine ». C'est une plateforme qui, dans le cadre de véhicules autonomes, permet de recueillir un panel des différentes visions culturelles de l'éthique vis-à-vis des décisions morales que l'Intelligence Artificielle pourra prendre. Plus

[59] Morgan Tual, « Polémique sur une étude affirmant qu'un programme peut repérer l'homosexualité sur le visage », 2017 https://www.lemonde.fr/pixels/article/2017/09/12/polemique-apres-une-etude-affirmant-qu-un-programme-peut-reperer-l-homosexualite-sur-le-visage_5184516_4408996.html

précisément, l'expérience propose à l'utilisateur d'effectuer un choix entre deux scénarios qui mettent en scène des accidents de la route inévitables. Le sujet doit alors trancher pour prendre la décision la plus « morale » entre une typologie de victime ou l'autre. Par exemple, il peut s'agir de sauver la vie de 2 personnes âgées de 80 ans se trouvant dans le véhicule autonome, ou bien de les « sacrifier » pour sauver la vie d'un enfant qui traverse au feu rouge.

Cette problématique qui consiste à savoir « qui choisir ? » s'explique dans un contexte où les voitures autonomes se développent de plus en plus ces dernières années. Lorsqu'un individu se trouve dans une situation « d'accident inévitable », il agira alors d'instinct, c'est-à-dire qu'il effectuera le choix proposé par le logiciel en une fraction de secondes sans penser aux conséquences qu'entrainerait son acte (sa propre mort, celle d'un autre usager…). Au contraire, une machine doit être programmée à l'avance pour parer à ce type de situations. Mais qui doit être sauvé ? Cette question implique de prendre en compte de nombreuses variables lors de la conception de ces véhicules.

Docteur en psychologie cognitive, Jean-François Bonnefon[60] est également président du groupe expert de la Commission Européenne sur l'éthique de la conduite autonome. Lors de son intervention sur la Moral Machine, il affirmait que la logique de l'éthique « conséquentialiste » voudrait épargner le plus grand nombre mais que « cela rentrerait en conflit avec des droits fondamentaux, comme celui de bénéficier d'une sécurité égale sur la route ». Il explique par ailleurs que cet enjeu constitue ce que l'on appelle un « dilemme social » en économie[61]. Selon lui, « les études de *Bonnefon, Shariff, Rahwan* (2016) illustrent l'inconfort que nous aurions à ôter la vie d'une petite fille au profit de deux personnes âgées, pourtant en surnombre ».

Cette expérience démontre que la présence de biais cognitifs au sein des programmes d'intelligence artificielle va poser des problèmes éthiques à l'échelle mondiale. Chaque culture ou politique possède une vision propre de la morale : ce qui peut être inenvisageable pour certains est admissible pour d'autres, tout dépend du référentiel dans lequel on se place. Ainsi, des programmes de voitures autonomes dont les décisions vont impacter la vie ou la mort d'individus à l'échelle mondiale en raison de sa commercialisation vont poser de nombreuses difficultés juridiques. Alors que le droit à la vie est un droit fondamental prévue

[60] Directeur de recherche au CNRS

[61] Louis Dumestre, « Éthique et Intelligence Artificielle : l'expérience « Morale Machine » », 2020, https://portail-ie.fr/analysis/2371/ethique-et-intelligence-artificielle-lexperience-morale-machine

à l'article 2 de la Convention européenne des droits de l'homme, la seule solution envisagée pour permettre le choix de sa propre vie au détriment de celle d'un autre est la légitime défense[62]. Qu'en sera-t-il de ce nouveau dilemme ?

En conséquent, il est nécessaire de prévenir les biais non désirés pour garantir des systèmes de confiance.

B) Une fiabilité incertaine des outils de reconnaissance biométriques

Certaines techniques numériques d'enquêtes acceptées et reconnues par la justice dans quelques pays sont remises en cause par la communauté scientifique. C'est le cas de la reconnaissance vocale considérée comme une caractéristique biométrique par le code de procédure pénale[63].

L'une des difficultés concerne la plateforme PNIJ dont il était question plus tôt. L'avantage procuré par la centralisation des interceptions judiciaires déploie dans le même temps des interrogations au regard des garanties de l'exercice des droits de la défense et du recueil et de l'usage des communications interceptées.

En effet, l'article R40-46 du CPP prévoit, selon une étude sur les enjeux des interceptions judiciaires dans la procédure pénale au prisme de la Plateforme nationale des interceptions judiciaires, la possibilité d'enregistrer les données de reconnaissance vocale de l'utilisateur et de les conserver jusqu'à la date de clôture des investigations en matière de communications électroniques et transmission de la procédure à l'autorité compétente[64]. Cette étude, menée par Clarisse Serre et Charles Evrard, affirme que « La PNIJ entérine le recours aux méthodes d'authentification vocale comme élément de preuve dans le cadre de la procédure pénale, et ce alors même que les spécialistes considèrent que la voix ne peut être considérée comme une donnée biométrique comme les autres en l'état des techniques actuelles »[65].

[62] Article 122-5 du CPP
[63] Article R40-46 CPP
[64] Article R. 40-49 CPP
[65] Clarisse Serre et Charles Evrard, « Du rififi chez les grandes oreilles », 2020, https://www.dalloz-actualite.fr/node/du-rififi-chez-grandes-oreilles

Pour affirmer cela, les juristes se fondent sur un article de Jean-François Bonastre, professeur au Laboratoire d'Informatique d'Avignon et spécialiste du traitement de la parole et de l'authentification vocale » intitulé « La voix n'est pas une biométrie classique ». Au sein de son étude, le professeur rappelle que la biométrie est définie comme « l'identification des personnes en fonction de caractéristiques biologiques ». Partant de cette constatation, selon lui, la voix n'est pas une biométrie : « par l'étude de la voix, nous ne mesurons pas une caractéristique biologique mais seulement la trace laissée par des mouvements d'airs causés par un phénomène de production vocale ».

Un autre exemple est développé par les auteurs, l'affaire du meurtre d'Elodie Kulik qui avait été enlevée, séquestrée, violée et tuée en 2002. La particularité de l'affaire réside dans le fait que son homicide a été enregistré lorsqu'elle a appelé les pompiers avec son téléphone portable après avoir eu un accident de voiture. La communication est établie pendant une durée de 26 secondes pendant lesquelles des cris de détresse sont entendus ainsi que les voix d'au moins deux hommes. Son corps est retrouvé brûlé le lendemain à 6 kilomètres du lieu de l'accident. La question que l'enquête devait résoudre était la suivante : peut-on déterminer quelles étaient les personnes présentes à l'aide de la reconnaissance vocale pour identifier les coupables ?

La première problématique fut la mauvaise qualité de la bande son et sa brièveté. Une comparaison automatique a donc été impossible à réaliser. Plusieurs proches de l'auteur ont alors été entendus pour identifier la voix du suspect Willy Bardon. Le premier expert, pour tester la fiabilité des réponses, leur a fait écouter des extraits de la voix de ce dernier parmi plusieurs autres. Au total, 6 personnes ont affirmé reconnaître la voix de Willy Bardon. Jean-François Bonastre, spécialiste de l'authentification des voix nommé précédemment, a pris la relève de l'expert quand ce dernier est mort sans avoir pu terminer sa mission.

Le professeur Bonastre démontre que le travail de son prédécesseur contient des erreurs, voire des mensonges et qu'il a utilisé des méthodes qui n'avaient pas été scientifiquement validées. Même s'il ne remet pas en question les témoignages en eux même, il affirme que l'humain a une capacité limitée à reconnaître une voix. « Je ne dis pas que ce n'est pas possible de reconnaître des voix à l'oreille. Mais ce n'est pas prouvé scientifiquement. »

Les réserves ainsi émises par le spécialiste démontrent que la reconnaissance vocale n'est pas une science exacte permettant de relier formellement un individu sur une scène de crime. En effet, comme le souligne le professeur, le phénomène de production vocale, qui se produit

lorsque l'on émet un son par la voix, est par nature unique et ne peut être reproduit. Ainsi, il est impossible d'obtenir 2 prélèvements de voix identiques et ce, même si le même mot a été prononcé 2 fois par la même personne. C'est en cela que l'empreinte vocale se différencie de l'empreinte digitale notamment. Plus précisément, les dessins papillaires provenant d'un doigt sont immuables c'est-à-dire qu'ils ne changent pas tout au long d'une vie. De cette manière, une preuve par reconnaissance vocale provenant d'une bande son ne peut pas être utilisée comme une empreinte digitale retrouvée sur une scène d'infraction. La première ne permet pas scientifiquement d'établir avec certitude la présence d'un individu sur les lieux tandis que la seconde le peut.

C'est pourquoi la voix fait partie de la catégorie des biométries « comportementales » et non des biométries dites « physiologiques » telles que la forme de la main, du doigt ou encore de l'œil. Les premières mesures les paramètres d'un comportement humain à l'instar de la marche, la voix et la frappe de clavier. Elles concernent des prélèvements qu'un individu peut modifier volontairement et par conséquent relèvent du domaine de la signature comportementale et non de l'empreinte. La seconde particularité de la biométrie comportementale est sa variabilité et qu'elle est variable et évolutive dans le temps.

Il est donc délicat que le code de procédure pénale adopte l'authentification vocale comme mode de preuve tandis que les avancées scientifiques ne l'admettent pas en tant que telle du fait de l'incertitude encore trop importante qui existe à son sujet. Sa variabilité et son évolutivité fond de la reconnaissance vocale une science plutôt incertaine qu'il est nécessaire de prendre en compte avec parcimonie sans faire d'elle une preuve irréfutable dans le cadre d'une enquête judiciaire.

Les technologies de reconnaissance faciale fonctionnant sur une méthode statistique peuvent aussi comporter des failles inextricablement liées aux biais algorithmiques présentés précédemment. Ainsi, cet outil numérique peut être à l'origine de l'existence de « faux positifs », c'est-à-dire que le logiciel va identifier une personne comme la personne recherchée à partir de la base de données photographique alors que ce n'est pas elle. A l'inverse, il existe aussi des « faux négatifs » lorsque le programme ne reconnaît pas la présence d'une personne sur les données comparées alors que celle-ci s'y trouve effectivement.

Cette conséquence découle de l'existence de biais algorithmiques présents à l'intérieur du programme. Ainsi, si le logiciel est moins précis pour la reconnaissance de visages noirs en raison d'un biais discriminatoire, il conduira à l'apparition de faux positifs plus facilement chez les personnes noires. De cette manière, un encadrement permettant de prévenir l'existence de biais amènera dans le même temps la disparition de certaines erreurs du dispositif.

Chapitre 2) Limitation européennes des techniques d'enquêtes numériques

Les progrès permis par le développement massif des technologies numériques au sein des enquêtes judiciaires se trouvent contrebalancés par les dangers qui en découlent. C'est dans le but de limiter ces risques que l'emploi des nouvelles techniques d'enquêtes est encadré juridiquement au niveau National ainsi qu'au niveau Européen (section 1). Ce cadre juridique permet notamment à l'Etat de prévenir des atteintes aux libertés individuelles mais aussi les dérives potentielles de l'intelligence artificielle (section 2).

Section 1_ Encadrement juridique National et Européen des technologies numériques au sein des enquêtes judiciaires

En France, si les technologies numériques ont été largement intégrées comme outil au sein des enquêtes judiciaires, leur utilisation est quant à elle strictement limitée. Leur encadrement strict s'explique tout d'abord en raison du système institutionnel en vigueur qu'est l'Etat de droit (§1) mais aussi du contexte européen dans lequel l'Union européenne contraint les Etats membres à transposer ses directives dans le droit national (§2).

§1 : Un emploi juridiquement limité en France

A) Un encadrement strict dans le contexte d'un Etat de droit

1. Le cas particulier du contexte français

Le code pénal définit l'acte terroriste comme un acte se rattachant à « *une entreprise individuelle ou collective ayant pour but de troubler gravement l'ordre public par l'intimidation ou la terreur* ». De plus, l'article 29 du traité de l'Union européenne qualifie le terrorisme d'une forme grave de criminalité qu'il est nécessaire de prévenir au niveau de l'Union.

C'est pourquoi les attentats terroristes ébranlent notre société plus que la délinquance en col blanc ou la criminalité organisée dites plus « classiques ». Ils remettent en question à la fois notre sécurité que l'on croyait acquise mais aussi, par conséquent, nos libertés individuelles et collectives. Prenons pour premier exemple les attentats du 13 novembre 2015 perpétrés à Paris et à Saint Denis. Au total, 131 personnes ont perdu la vie et 250 ont été blessées.

Cet épisode d'une rare violence a terrorisé non seulement les survivants de cette soirée mais aussi la France entière. Comment les citoyens peuvent-ils se sentir en sécurité dans les rues publique après un tel massacre ? La réponse est délicate, une attaque de cette ampleur expose l'échec cuisant de l'Etat à assurer la sécurité nationale. Sécurité qui nous est assurée, selon lui, en échange d'une certaine limitation de nos droits et libertés. C'est la raison pour laquelle les attentats commis sur le territoire national ont profondément bouleversé la Nation française.

Le second exemple est relatif à l'exercice de la liberté d'expression et concerne les attentats contre Charlie Hebdo. C'est une attaque terroriste islamiste qui a été perpétuée contre le journal satirique dénommé « Charlie Hebdo » le 7 janvier 2015, à Paris. Ce journal fait quotidiennement la critique de la religion et, en particulier, des intégristes religieux. Il avait été la cible de nombreuses menaces des islamistes auparavant. Les terroristes ont tenté de réduire au silence les rédacteurs par la violence. Cette illustration expose une autre faillite de l'Etat dans son engagement pour garantir le libre exercice de la liberté d'expression. Désormais, les citoyens ont conscience que, si leurs droits et libertés sont restés intacts, leur exercice demeure risqué.

Ces évènements tragiques ont conduit les différents gouvernements à renforcer les dispositifs de sécurité et d'enquête empiétant nécessairement sur les libertés individuelles dans un objectif de prévention des futurs attentats.

L'encadrement « strict » qui en découle s'explique par l'histoire de France et de ses institutions. Pour comprendre cela, il faut remonter à la Déclaration des droits de l'homme et du citoyen (DDHC). Résultat de la volonté du peuple, représentée par l'Assemblée constituante, elle fait suite à la Révolution française. Adoptée le 26 aout 1789, elle définit des droits « naturels et imprescriptibles » de l'homme que sont la liberté, la propriété, la sûreté et la résistance à l'oppression. Elle reconnaît ainsi l'égalité devant la loi et la justice et affirme le principe de séparation des pouvoirs.

Dans un contexte postrévolutionnaire, les représentants du Peuple Français affirment leurs revendications dans le préambule comme suit « considérant que l'ignorance, l'oubli ou le mépris des droits de l'Homme sont les seules causes des malheurs publics et de la corruption des Gouvernements, ont résolu d'exposer, dans une Déclaration solennelle, les droits naturels, inaliénables et sacrés de l'Homme, afin que cette Déclaration, constamment présente à tous les Membres du corps social, leur rappelle sans cesse leurs droits et leurs devoirs ; afin que les actes du pouvoir législatif, et ceux du pouvoir exécutif, pouvant être à chaque instant comparés avec le but de toute institution politique, en soient plus respectés ; afin que les réclamations des citoyens, fondées désormais sur des principes simples et incontestables, tournent toujours au maintien de la Constitution et au bonheur de tous »[66].

Encore présent dans le droit positif, elle fait désormais partie du préambule de la Constitution et a été reconnue par le Conseil constitutionnel en 1971 comme ayant valeur constitutionnelle.

C'est un héritage qui a marqué l'histoire de la France que les constituants souhaitent perpétuer et ne pas oublier. La Déclaration universelle des droits de l'homme du 10 décembre 1948 mais aussi la Convention européenne des droits de l'homme du 4 novembre 1950 revendiquent ce même héritage.

C'est la raison pour laquelle, l'Etat français attache tant d'importance à la préservation des droits et libertés fondamentaux. Marqué par son passé, impacté d'une manière différente que

[66] Assemblée Nationale, Déclaration des Droits de l'Homme et du Citoyen de 1789, 1798 https://www.legifrance.gouv.fr/contenu/menu/droit-national-en-vigueur/constitution/declaration-des-droits-de-l-homme-et-du-citoyen-de-1789

les autres pays, de nombreux outils numériques ne sont pas employés par les enquêteurs parce que leur mise en œuvre est trop attentatoire. C'est le cas, notamment, de la reconnaissance faciale ou encore de l'usage des drones dans les villes.

C'est dans ce but de protection que l'Etat s'est évertué à ériger de nombreux boucliers, dans le but de prévenir des atteintes disproportionnées aux droits et libertés pour garantir la sécurité publique. L'organe principal assurant le respect de cette obligation est le Conseil constitutionnel. Créé par le constituant de 1958, il est chargé de vérifier la conformité des lois aux différents principes constitutionnels. L'esprit du Conseil était de préserver les prérogatives de l'exécutif de l'empiètement des assemblées tout en contenant les majorités politiques dans les limites de la Constitution.

Sa création résulte de longs débats et réflexions sur la nécessité de fonder un contrôle de la loi qui protégerait les principes fondamentaux du régime. Ce système de contrôle de la constitutionnalité des lois permet de développer considérablement les principes de fond ainsi que de les imposer efficacement au législateur.

De ce fait, le législateur a le devoir de concilier sa mission de prévenir et réprimer efficacement pour garantir la sureté des personnes avec le respect des libertés individuelles que la délinquance met en danger. Ce principe de proportionnalité a pour objectif d'imposer un seuil que les Etats ne doivent pas dépasser concernant les droits des personnes, fusse-t-il franchit au nom de la défense Nationale et de la sécurité.

2. Un encadrement législatif strict

Si l'utilisation de certains outils numériques particulièrement attentatoires aux libertés individuelles a été intégrée aux moyens d'investigations, son champ d'application est toujours restreint aux infractions les plus graves ou ciblées en raison de la difficulté d'obtention de preuves dans un domaine[67]. C'est notamment le cas des techniques spéciales d'enquêtes[68] qui ne peuvent être employées que dans le cadre de certaines infractions préalablement spécifiée. En effet, cela concerne uniquement les infractions de délinquance et criminalité organisée[69].

[67] La cybercriminalité par exemple.
[68] Prévues aux articles 760-95-1 et suivants du CPP
[69] Articles 706-73 et 706-73-1 du CPP

Ces dispositifs sont ainsi limités quant à leur finalité. Les techniques spéciales d'enquête comportent un deuxième élément qui est cumulatif au premier : la nécessité. C'est-à-dire qu'elles doivent être utilisées pour répondre aux besoins d'une enquête ou d'une instruction. Quant à l'usage de la reconnaissance faciale, du fait de leur qualification de « données sensibles » et de la directive dite « police justice », l'emploi de ces données biométrique est aussi strictement encadré. En principe interdite, elle fait l'objet d'un régime d'exception et peut être employée dans quatre situations : lorsque la personne concernée consent explicitement à son utilisation, lors de son utilisation pour des motifs d'intérêts public, lorsque les données traitées sont manifestement rendues publiques par la personne concernée, lors de l'exercice ou la défense d'un droit en justice.

Un dernier exemple concerne l'emploi de drones. En effet, depuis la loi du 24 janvier 2022[70], leur utilisation doit permettre d'atteindre l'une des finalités prévue par l'article L242-5 du code de la sécurité intérieure, c'est à dire « la prévention des atteintes à la sécurité des personnes et des biens dans des lieux particulièrement exposés », « la sécurité des rassemblements de personnes sur la voie publique ou dans des lieux ouverts au public ainsi que l'appui des personnels au sol », « la prévention d'actes de terrorisme », « la régulation des flux de transport », « la surveillance des frontières » et enfin « le secours aux personnes ». Par ailleurs, leur usage doit être proportionné à la finalité poursuivie.

De surplus, le cadre d'utilisation comporte nécessairement de nombreuses garanties procédurales. L'emploi de ces technologies numériques implique nécessairement une autorisation préalable par des autorités judiciaires différentes des enquêteurs. Cette autorisation, pour l'usage de drones dans la conduite d'enquêtes est, depuis la loi du 24 janvier 2022, « délivrée par décision écrite et motivée du représentant de l'Etat dans le département ou, à Paris, du préfet de police ». Pour les techniques spéciales d'enquête, l'autorisation doit être délivrée par le juge des libertés et de la détention à la requête du procureur de la République au cours de l'enquête ou par le juge d'instruction, après avis du procureur de la République au cours de l'information. Ainsi seuls des magistrats du siège sont compétents. Ce sont, dans ces deux situations, des autorités indépendantes qui permettent d'appliquer une garantie supplémentaire.

[70] Loi n° 2022-52 adaptant le régime juridique des drones aux recommandations de la décision du Conseil constitutionnel n° 2021-817 DC du 20 mai 2021

Leur champ d'application est aussi limité dans le temps et dans l'espace. L'encadrement concerne donc aussi la durée de l'autorisation, sa mise en place, le traitement des enregistrements mais prévoit aussi la destruction des données recueillis. Ainsi, l'autorisation d'utilisation des techniques spéciales d'enquête au cours d'une enquête est délivrée pour une durée d'un mois renouvelable[71].

Dans le cadre de l'utilisation d'un dispositif aéroporté, il est prévu que l'autorisation préfectorale ne peut « excéder le périmètre géographique strictement nécessaire à l'atteinte de cette finalité » dans un objectif de respect du principe de proportionnalité. De plus, leur utilisation permanente est interdite, c'est pourquoi l'article prévoit que l'autorisation est délivrée pour une durée maximale de trois mois, et renouvelable selon les mêmes conditions. Elle doit préciser le nombre maximal de caméras pouvant procéder simultanément aux enregistrements au regard des autorisations qui ont déjà été délivrées dans ce périmètre.

Enfin, le recours aux dispositifs numériques présente des garanties procédurales qui concernent le respect de la vie privée. C'est pourquoi, dans le cadre de l'emploi de techniques spéciales d'enquêtes, 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. Qui plus est, les enregistrements et données recueillis lors des opérations effectuées sont détruits à l'expiration du délai de prescription de l'action publique.

Concernant les dispositifs aéroportés, l'article L242-4 prévoit que lors de la mise en œuvre de ce dispositif « Les dispositifs aéroportés ne peuvent ni procéder à la captation du son, ni comporter de traitements automatisés de reconnaissance faciale ». Les modalités d'utilisation et de conservation des données personnelles collectées est prévue par ce même article. En effet, « Ces dispositifs ne peuvent procéder à aucun rapprochement, interconnexion ou mise en relation automatisé avec d'autres traitements de données à caractère personnel ».

De la même manière, il est ainsi interdit de recueillir des images captant l'intérieur d'un domicile privé ainsi que son entrée. Si la situation se produit, l'enregistrement doit être immédiatement interrompu. Si tel n'a pas pu être le cas, les images doivent être effacées dans un délai de quarante-huit heures. Enfin, les enregistrements comportant des données à caractère personnel sont conservés pendant une « durée maximale de sept jours à compter

[71] A la différence de l'autorisation dans le cadre d'une information judiciaire qui est délivrée pour une durée maximale de quatre mois, renouvelable dans les mêmes conditions de forme et de durée.

de la fin du déploiement du dispositif, sans que nul ne puisse y avoir accès, sauf pour les besoins d'un signalement dans ce délai à l'autorité judiciaire ».

Ces restrictions s'expliquent par l'atteinte aux libertés individuelles que ces dispositifs engendrent indéniablement. Leur limitation, comme expliqué précédemment, fait l'objet d'un contrôle de proportionnalité entre l'objectif de sécurité publique et le respect des libertés individuelles.

B) Encadrement juridique Européen

Reconnaissance faciale. L'utilisation de dispositifs de reconnaissance faciale représente une ingérence au regard des article 8 (droit à la protection des données) et 7 (droit à la vie privée) garantis par la charte des droits fondamentaux de l'Union européenne en raison du traitement des données à des fins d'identification. L'enregistrement, la conservation et la comparaison à des fins d'identification implique une restriction de ces droits fondamentaux qui, à ce titre, doit être strictement nécessaire et proportionnée[72].

En vertu des principes juridiques primordiaux en matière de protection des données, prévus par l'article 5 du RGPD et l'article 4 de la directive UE 2016/680, le traitement des images faciales doit respecter plusieurs conditions. Tout d'abord, il doit être licite, loyal et transparent. Pour la vidéosurveillance, au titre du RGPD, le comité européen de la protection des données recommande la cumulation de deux conditions pour se conformer aux exigences en matière de transparence. Les informations les plus importantes doivent être fournies par la présence d'un panneau d'avertissement placé pour que « la personne concernée puisse aisément reconnaître les circonstances de la surveillance avant de pénétrer dans la zone surveillée ». D'autres indications obligatoires peuvent être transmises par le biais de divers moyens accessibles, comme une affiche ou un site internet. Le Conseil de l'Europe choisit, de la même manière, différents niveaux de transparence dans ses lignes directrices sur la reconnaissance faciale. De même, il adopte une approche à plusieurs niveaux dans ses recommandations.

[72] Article 52, paragraphe 1 de la charte des droits fondamentaux de l'UE.

Concernant la loyauté, le comité européen de la protection des données a considéré, dans ses lignes directrices, que la « loyauté est un principe fondamental selon lequel les données à caractère personnel ne doivent pas être traitées d'une manière injustifiablement préjudiciable ou illégalement discriminatoire, inattendue ou trompeuse pour la personne concernée ».

Ensuite, le dispositif doit nécessairement suivre une finalité déterminée, explicite et légitime c'est-à-dire clairement définie dans le droit de l'État membre ou de l'Union. Le principe est qu'un traitement ultérieur des données dans un objectif incompatible avec sa finalité prédéterminée n'est possible que dans des conditions de l'article 5 du RGPD, et de l'article 4 de la directive 2016/680. Cette finalité doit être exprimée de façon précise de manière à ce que la personne concernée la comprenne.

Pour prévenir des risques de détournement d'usage de ces logiciels, c'est-à-dire leur utilisation pour des finalités interdites, il est recommandé que les systèmes et les processus associés inclus des garanties.

Enfin, ce traitement d'images faciales doit être conforme aux exigences de minimisation des données, d'exactitude des données, de limitation de la conservation, de sécurité des données et de responsabilité.

Selon le parlement européen[73], le principe de minimisation des données est généralement interprété comme « signifiant que la quantité de données devrait être limitée (RGPD) à ce qui est nécessaire ou non excessive au regard des finalités pour lesquelles elles sont traitées [article 5, paragraphe 1, point c), du RGPD, et article 4, paragraphe 1, point c), de la directive (UE) 2016/680] ». L'anonymisation des données pourrait être une solution si la situation le permet.

Le principe prévoit que les données ne soient pas conservées de façon à permettre l'identification des personnes concernées pour une durée supérieure au regard des finalités pour lesquelles ces données sont traitées[74]. De plus, ces dernières doivent être « exactes factuellement et temporellement » ce qui signifie qu'elles doivent être mises à jour régulièrement. Un arrêt de la Cour de Justice de l'Union européenne affirme cependant que le « caractère exact et complet de données à caractère personnel doit être apprécié au regard

[73] Parlement européen, « Règlementation de la reconnaissance faciale au sein de l'Union européenne », 2021, https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/698021/EPRS_IDA(2021)698021_FR.pdf
[74] Idem

de la finalité pour laquelle ces données ont été collectées »[75]. Certaines erreurs pourraient ainsi être tolérées à cet égard.

De plus, dans un objectif de lutte contre les biais, le Conseil de l'Europe prévoit que les développeurs « devront éviter les erreurs d'étiquetage en testant suffisamment leurs systèmes et en identifiant et éliminant les disparités dans la précision, notamment en ce qui concerne les variations démographiques de la couleur de la peau, l'âge et le sexe, et éviter ainsi toute discrimination involontaire »[76].

Ensuite, les données doivent être traitées de façon à « garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées ». Cette garantie est prévue dans le but de respecter le principe de sécurité des données.

Enfin, le respect d'un principe de responsabilité prévoit que le responsable du traitement effectue une analyse complète concernant l'admissibilité juridique et les risques associés à la mise en place de ces dispositifs.

De cette manière, le Conseil de l'Europe a assorti la possibilité d'emploi de ce dernier par les Etats membres de plusieurs garanties légales. Plus avancée que la France en matière de règlementation de la reconnaissance faciale pour un usage par les forces de police, l'Union européenne a limité son utilisation pour garantir le respect des droits et libertés fondamentaux.

[75] Arrêt de la CJUE du 20 décembre 2017, affaire C434/16, Nowak
[76] Idem 74

§2 : Des évolutions juridiques envisagées pour s'adapter aux défis du numérique

A) Les évolutions envisagées à l'échelle nationale

Le droit doit constamment s'adapter aux évolutions de la société : à la nécessité d'instaurer des nouvelles normes et celle d'adapter les normes préexistantes. L'explosion des technologies numériques de l'information et de la communication nous a conduit vers l'apparition de nouvelles formes de délinquance.

C'est pourquoi un projet de loi est prévu par le ministère de l'Intérieur, intitulé « Projet de loi d'orientation et de programmation du ministère de l'Intérieur » (LOPMI). Le ministère de l'Intérieur doit répondre aux enjeux sécuritaires et territoriaux des années à venir, en dotant « le ministère de l'intérieur de nouveaux moyens humains, juridiques et budgétaires ». Il affirme notamment que « Répondre aux défis présents et à venir suppose de prendre le tournant révolutionnaire du numérique, d'agir dans la proximité et de mieux prévenir les crises futures. »

Il est prévu que la LOPMI donnera également les moyens de mieux faire face aux crises (ordre public, délinquance et criminalité, crises de sécurité civile). Selon le ministère, « Répondre mieux qu'hier à la délinquance du quotidien et à la criminalité suppose ainsi de continuer de renforcer les moyens d'investigation ».

L'un des objectifs principaux de ce projet est de doter les forces de sécurité d'un équipement à la pointe du numérique. Pour ce faire, il est prévu que soit créé une agence du numérique des forces de sécurité, d'augmenter les forces de sécurité et de secours avec des équipements innovants tels que des caméras-piétons, des caméras embarquées dans les véhicules, des terminaux numériques et des postes mobiles permettant l'accès à toutes les ressources utiles depuis le terrain. Enfin, il est prévu de moderniser et mutualiser les infrastructures de communication en déployant le « réseau radio du futur », commun aux forces de sécurité et de secours, et le projet « NexSIS », pour mutualiser la gestion des alertes des services

d'incendie et de secours[77]. Le déploiement des drones est aussi prévu, en appui opérationnel ou pour le recueil de renseignement.

L'amélioration des moyens d'investigations n'est cependant pas suffisante pour garantir la mise en place d'enquêtes plus performantes. Pour cette raison, il est prévu d'augmenter de 50 % le temps de formation initiale et continue des policiers et gendarmes. Ceci, par le biais du recrutement de 1 500 formateurs et la création de nouvelles écoles spécialisées pour les forces de sécurité telles qu'une école du cyber, une académie de police et un centre de formation au maintien de l'ordre.

Plan France 2030. Le président de la République, Emmanuel Macron, a également décidé de s'engager dans la voie de l'intelligence artificielle notamment au moyen du plan France 2030. Selon le ministère de l'économie, des finances et de la souveraineté industrielle et numérique, l'objectif principal est de devenir pionnier de l'innovation et, pour ce faire, le gouvernement a lancé une stratégie nationale pour l'intelligence artificielle en 2018 divisée en deux phases.

La première, dotée d'un investissement de 1,5 milliards d'euros entre 2018 et 2022, tendait à positionner la France comme un leader mondial des disciplines scientifiques ainsi que des technologies du traitement de l'information[78]. La stratégie envisagée est de favoriser « la création et le développement d'un réseau d'instituts interdisciplinaires d'intelligence artificielle, le soutien à des chaires d'excellence en IA, le financement de programmes doctoraux et l'investissement dans les capacités de calcul de la recherche publique »[79].

La seconde phase de cette stratégie nationale de l'IA a été lancée par le Gouvernement le 8 novembre 2021, dont le but est d'augmenter le nombre de talents formés dans ce domaine d'innovation et d'accélérer le potentiel de la recherche et du développement en succès économiques. Il est prévu un budget de 2,22 milliards d'euros pour les cinq prochaines années.

[77] Ministère de l'intérieur, « Projet de loi d'orientation et de programmation du ministère de l'intérieur 2022-2027 », 2022, https://www.interieur.gouv.fr/sites/minint/files/medias/documents/2022-03/16-03-2022-projet-de-loi-d-orientation-et-de-programmation-du-ministere.pdf

[78] Ministère de l'économie, des finances et de la souveraineté industrielle et numérique, La stratégie nationale pour l'intelligence artificielle, 2021, https://www.economie.gouv.fr/strategie-nationale-intelligence-artificielle

[79] Bis 75

La stratégie est pilotée par le coordinateur national pour l'intelligence artificielle Renaud Vedel, et s'inscrit dans la gouvernance des crédits du Programme d'investissements d'avenir (PIA) et France 2030 par le Secrétariat général pour l'investissement (SGPI).

Quelques exemples des objectifs fixés pour atteindre ce but sont, notamment, la formation et le financement d'une cible d'au moins 2000 étudiants en DUT, licence et licence pro. Cette ligne directrice concerne également la formation de 1500 étudiants en master et 200 thèses supplémentaires par an à un rythme régulier.

La deuxième phase c'est aussi la volonté de placer au minimum 1 établissement d'excellence dans les meilleurs rangs internationaux. Enfin, le gouvernement prévoit le recrutement de 15 scientifiques étrangers d'envergure mondiale d'ici janvier 2024[80].

B) Les évolutions envisagées à l'échelle européenne

Afin de renforcer la compétitivité de l'Union européen ainsi que de garantir la confiance dans ses valeurs, la Commission facilite d'ores et déjà la coopération en matière d'intelligence artificielle. En 2018, elle publie sa stratégie européenne sur l'IA qui est composée de 52 experts indépendants spécialisés dans l'industrie, la société civile et le monde universitaire.

Ce groupe a déjà publié un projet formant les lignes directrices, selon la Commission, en matière d'éthique la même année. Des consultations des parties et des réunions avec des représentants ont ensuite été organisées.

En s'appuyant sur les travaux de ces experts indépendants, le 8 avril 2019, la Commission européenne a lancé une initiative d'élaboration d'un consensus international pour une Intelligence Artificielle centré sur l'humain et des valeurs essentielles que sont la dignité, la sécurité, l'indépendance et la liberté. Ce projet a pour objectif d'augmenter les investissements publics et privés pour qu'ils atteignent 20 milliards d'euros par an au cours

[80] Bruno Le Maire, Frédérique Vidal et Cédric O, « Stratégie nationale pour l'intelligence artificielle – 2e phase : Conquérir les talents et transformer notre potentiel scientifique en succès économiques », 2021, https://minefi.hosting.augure.com/Augure_Minefi/r/ContenuEnLigne/Download?id=334FD34F-7844-497E-9551-79EDFF3B2EEF&filename=1645%20-%20DP%20-%20Strat%C3%A9gie%20Nationale%20pour%20l%27IA%202%C3%A8me%20phase.pdf

des dix prochaines années. Cela permettra d'accroître le volume des données disponibles, de favoriser les talents et de garantir la confiance.

Il est désormais reconnu que l'Intelligence artificielle peut s'avérer bénéfique dans de nombreux secteurs comme les soins de santé, la sécurité des véhicules, la gestion des risques financiers mais permet aussi aux autorités répressives de lutter plus efficacement contre la criminalité. La commission a fait le choix d'organiser son plan d'action en trois étapes : définir les exigences clés pour une IA digne de confiance, lancer une phase pilote à grande échelle pour recueillir les réactions et retours d'informations des parties prenantes, et élaborer un consensus international pour une IA centrée sur l'humain[81].

La Commission prévoit sept éléments pour parvenir à une IA de confiance. Elle les énumère de la manière suivante :

Le « facteur de l'humain et du contrôle humain » c'est-à-dire que « les systèmes d'IA devraient être les vecteurs de sociétés équitables en se mettant au service de l'humain et des droits fondamentaux, sans restreindre ou dévoyer l'autonomie humaine ».

Le second élément correspond à la Robustesse et la sécurité de l'IA. Ainsi, « une IA digne de confiance nécessite des algorithmes suffisamment sûrs, fiables et robustes pour gérer les erreurs ou les incohérences dans toutes les phases du cycle de vie des systèmes d'IA ».

Ensuite sont visés à la fois le respect de la vie privée et la gouvernance des données. Dans cette optique, « il faut que les citoyens aient la maîtrise totale de leurs données personnelles et que les données les concernant ne soient pas utilisées contre eux à des fins préjudiciables ou discriminatoires ».

La transparence doit aussi être assurée notamment par la « traçabilité des systèmes d'IA ».

La Commission défend aussi la diversité, la non-discrimination et l'équité. Elle souhaite que les systèmes d'IA prennent en compte toutes les capacités, aptitudes et besoins humains ainsi que leur accessibilité soit garantie.

[81] Commission Européenne, « Intelligence artificielle : la Commission franchit une étape dans ses travaux sur les lignes directrices en matière d'éthique », 2019, https://ec.europa.eu/commission/presscorner/detail/fr/IP_19_1893

Elle promeut le « Bien-être sociétal et environnemental » en proposant que les systèmes d'IA soient utilisés « pour soutenir des évolutions sociales positives et renforcer la durabilité et la responsabilité écologique ».

Enfin, l'IA doit être pensée dans un objectif de responsabilisation. Il convient alors, selon la Commission, « de mettre en place des mécanismes pour garantir la responsabilité à l'égard des systèmes d'IA et de leurs résultats, et de les soumettre à une obligation de rendre des comptes ».

Concernant la deuxième phase prévue qui a d'ores et déjà débutée, les partenaires ont déjà commencé à adhérer l'Alliance européenne pour l'IA. C'est un forum engagé dans une discussion large et ouverte sur tous les aspects du développement de l'intelligence artificielle et de son impact[82]. Cette plateforme encourage la participation au processus d'élaboration des politiques de la Commission européenne.

Enfin, la dernière étape de son plan est l'élaboration d'un consensus international pour une IA axée sur le facteur humain. En d'autres termes, la Commission souhaite porter son projet sur la scène internationale, notamment en renforcer sa coopération avec les partenaires qui partagent les mêmes idées sur l'IA. Elle participe activement, dans ce but, aux discussions et initiatives internationales[83].

Le 21 avril 2021, la Commission européenne a présenté une proposition de règlement concernant les risques liés à l'Intelligence Artificielle. En tant que premier cadre juridique en matière d'Intelligence Artificielle, il permettrait à l'Europe de jouer un rôle primordial à l'échelle mondiale. Dans l'objectif de traiter ces dangers, le règlement les classe en quatre niveaux différents : risque minime, risque limité, risque élevé et enfin risque inacceptable.

La Commission expose précisément ses objectifs :

« Veiller à ce que les systèmes d'IA mis sur le marché de l'Union et utilisés soient sûrs et respectent la législation en vigueur en matière de droits fondamentaux et les valeurs de l'Union ;

[82] Commission européenne, « L'Alliance européenne de l'IA, 2022 », https://digital-strategy.ec.europa.eu/fr/policies/european-ai-alliance

[83] Notamment au sein du G7 et du G20

Garantir la sécurité juridique pour faciliter les investissements et l'innovation dans le domaine de l'IA ;

Renforcer la gouvernance et l'application effective de la législation existante en matière de droits fondamentaux et des exigences de sécurité applicables aux systèmes d'IA ;

Faciliter le développement d'un marché unique pour des applications d'IA légales, sûres et dignes de confiance, et empêcher la fragmentation du marché. »

La CNIL, ses homologues ainsi que le Contrôleur européen de la protection des données ont publié un avis sur la proposition de règlement précitée le 18 juin 2021. Elle relève 4 points centraux, tout d'abord « la nécessité de tracer des lignes rouges aux futurs usages de l'IA ». En effet, la CNIL accueille positivement la décision de la Commission de préciser les emplois interdits pour construire une Intelligence artificielle éthique ainsi que de confiance au sein de l'Union Européenne. Dans cet avis est toutefois souligné l'importance d'élargir le domaine d'interdiction des systèmes d'intelligence Artificielle mais aussi d'éclaircir leur définition.

La Commission souligne un deuxième point relatif au défi que représente son articulation avec le RGPD. Elle affirme que « compte tenu des risques extrêmement élevés posés par l'identification biométrique à distance des personnes dans les espaces publics (reconnaissance des visages, de la démarche, des empreintes digitales, de la voix, etc.) », les exceptions à l'interdiction générale devraient être supprimées. Dans cet avis, la CNIL « recommande également une interdiction des systèmes biométriques utilisés aux fins de classer les individus dans des groupes basés sur l'ethnicité supposée, le sexe, l'orientation politique ou sexuelle, ou d'autres motifs pour lesquels la discrimination est interdite en vertu de l'article 21 de la Charte des droits fondamentaux de l'Union européenne. L'utilisation de systèmes d'IA pour déduire les émotions d'une personne physique est par ailleurs considérée comme hautement indésirable et devrait également être soumise à une interdiction de principe (sauf cas très spécifiques, tels que certains objectifs de santé). Enfin, les systèmes utilisés pour la notation sociale (« social scoring ») doivent être systématiquement interdits. »

De cette manière, elle souhaite restreindre la volonté de la Commission européenne de donner la possibilité aux Etats d'employer, sous certaines conditions, ces technologies numériques. En effet, bien que ces dernières permettraient de révolutionner les enquêtes pénales et les capacités de résolution de celles-ci, leur impact principal serait la réduction des libertés individuelles. C'est pourquoi la CNIL, en tant qu'autorité de protection des données ne peut permettre qu'un tel recul ait lieu, fusse-t-il justifié par un objectif de sécurité publique. Cependant, nous verrons plus loin que les systèmes d'Intelligence Artificielle tels qu'employés dans le cadre d'une notation sociale peuvent être dangereux notamment dans des pays peu protecteurs des libertés individuelles (Section 2, §2, A).

Cet avis consultatif prend ainsi position face aux technologies d'IA en plaçant les barrières pour prévenir des risques d'utilisation future de ces différents outils.

Section 2_ Une limitation nécessaire à la prévention des atteintes aux droits et libertés

L'utilisation des outils numériques dans les enquêtes pénales entraine nécessairement une atteinte aux libertés individuelles principalement par leur intrusion dans la vie privée des personnes qui en font l'objet (§1). Les risques engendrés par l'emploi de ces technologies modernes ne s'arrêtent cependant pas là, certains découlent des failles résultant de l'essence même de l'Intelligence Artificielle exploitée (§2).

§1 Le risque de développement des techniques d'enquêtes au détriment des libertés individuelles

A) Une mise en balance des enjeux entre sécurité et liberté

Les possibilités d'amélioration des enquêtes judiciaires par le biais des technologies numériques présentent un atout majeur dans la lutte contre la délinquance. C'est pourquoi, le développement de cet emploi permettra d'assurer plus efficacement la protection de l'ordre public. Cependant, cette évolution ne doit pas se faire au détriment des libertés individuelles qui doivent faire l'objet d'une protection accrue. En France, sont aujourd'hui prévus plusieurs boucliers permettant de défendre les libertés individuelles et collectives face à la promulgation de lois trop attentatoires.

En effet, prévu par la constitution de 1958, le Conseil constitutionnel, garant des libertés individuelles et contrôleur de la constitutionnalité des lois, assure un contrôle de proportionnalité entre ces deux objectifs que doit poursuivre le législateur. Plus précisément, il doit trouver un équilibre en encadrant strictement le recours aux technologies numériques permettant de justifier les atteintes par un objectif de sécurité qui le nécessite.

Ainsi, le Conseil est intervenu très régulièrement, a priori, lors de la promulgation de lois autorisant l'utilisation de technologies d'enquêtes modernes. Ce fut le cas concernant l'usage de dispositifs aéroporté.

Dans sa décision du 20 mai 2021[84], il a censuré les dispositions des articles 41, 47 et 48 de la loi n° 2021-646 du 25 mai 2021 pour une sécurité globale au motif que le législateur n'avait pas veillé à concilier les objectifs de valeur constitutionnelle que sont la prévention des atteintes à l'ordre public et de recherche des auteurs d'infractions avec le droit au respect de la vie privée.

Le Conseil a censuré des dispositions de l'article 47 qui déterminaient les conditions dans lesquelles les services de police et de gendarmerie devaient procéder au traitement d'images que les drones obtenaient au moyen de caméra embarquées. Selon lui, les garanties législatives étaient insuffisantes au regard de leur mobilité et de la hauteur à laquelle ils peuvent capter des images et sons. En effet, les drones peuvent capter des images de très nombreuses personnes mais aussi suivre leurs déplacements sur de longues distances. C'est la raison pour laquelle le Conseil estime que leur mise en œuvre doit être accompagnée de garanties particulières de nature à sauvegarder le droit au respect de la vie privée (§ 129 s). Le législateur doit donc déterminer précisément les finalités et les situations qui justifieraient le recours à ce type d'outil.

En effet, l'un des articles prévoyait leur mise en œuvre si la première condition concernant les nécessités « relatives à un crime ou à l'une des infractions entrant dans le champ d'application des articles 706-73 et 706-73-1 » l'exigeait. De cette manière, tous les crimes étaient concernés ce qui revenait à porter une atteinte disproportionnée au droit à la vie privée. C'est pourquoi le Conseil a censuré cette extension. Il a jugé que le législateur avait permis le recours à ces techniques d'enquête considérablement intrusives pour des infractions qui n'étaient pas nécessairement complexes, et ce, « 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 ».

Cette décision est essentielle au sens où il a été rappelé l'importance d'effectuer la balance entre la réponse judiciaire et le respect des libertés individuelles. Selon les mots du Conseil, le législateur n'a pas effectué une « conciliation équilibrée entre, d'un côté, l'objectif de recherche des auteurs d'infractions et, de l'autre, le droit au respect de la vie privée, le secret des correspondances et l'inviolabilité du domicile ».

[84] Décision n° 2021-817 DC

De cette manière, le Conseil est un garant des libertés individuelles comme la liberté d'aller et venir et la liberté d'expression mais aussi collectives telles que la liberté de manifester et d'association par exemple.

Aux côtés du Conseil constitutionnel est apparu un autre organe de protection des données à caractère personnel avec le développement des nouvelles technologies de l'information et des télécommunications : la CNIL. Appelée Commission nationale de l'informatique et des libertés, créée en 1973, son rôle est d'informer et de conseiller le grand public mais aussi de contrôler les organismes et de régulation réguler leur usage des données personnelles[85].

La CNIL peut notamment contrôler les organismes et, en cas de manquements constatés, elle possède un pouvoir de sanction après mise en demeure. Elle exerce un contrôle a posteriori de la mise en œuvre concrète des lois. Elle constitue un moyen privilégié d'intervention auprès des responsables de traitement de données personnelles. Selon la CNIL, le programme des contrôles est élaboré en fonction de l'actualité et des problématiques dont elle est saisie[86].

Elle exerce une activité d'innovation et de prospective. De cette manière elle participe à la constitution de débats de société sur les enjeux éthiques des données. Elle assure un point de contact et de dialogue avec les systèmes d'innovation tels que les chercheurs et start-up. De plus, elle contribue à l'élaboration de solutions technologiques qui soient protectrices de la vie privée en conseillant les entreprises le plus tôt possible[87].

La loi du 7 octobre 2016, pour une République numérique, a confié à la CNIL la mission de développer « une réflexion sur les enjeux éthiques et les questions de société soulevés par l'évolution des technologies numériques »[88].

Dans le but de contribuer aux débats sur le numérique, la CNIL a lancé l'espace éditorial appelé LINC. On y retrouve des éclairages et réflexions prospectives ainsi que des partages et expérimentations.

---

[85] Olivier Aim « Les théories de la surveillance - Du panoptique aux Surveillance Studies », *Armand Colin*, 2020

[86] CNIL, « Mission 4 - Contrôler et sanctionner », https://www.cnil.fr/fr/mission-4-controler-et-sanctionner

[87] CNIL, « Mission 3 - Anticiper et innover », https://www.cnil.fr/fr/mission-de-la-CNIL-anticiper-innovation

[88] CNIL, « Mission 3 - Anticiper et innover », https://www.cnil.fr/fr/mission-de-la-CNIL-anticiper-innovation

Lors du confinement général de la population française[89], la Commission a recensé une grande partie de l'arsenal qui a été mis en place par les pouvoirs publics. En 2020, au sein de plusieurs articles intitulés « le laboratoire d'innovation numérique de la CNIL » elle a énoncé les dangers potentiels de la gestion de la pandémie à travers les dispositifs de surveillance dont l'élaboration par le gouvernement avait été fait pour dépister la population et rendre visible le virus, sa contagion et le non-respect du confinement. Selon la elle, le danger principal est lié à la nature des outils numériques déployés pour remplir ses objectifs. Le risque est de rogner sur les libertés individuelles et collectives, tout en confisquant un trop grand nombre de données personnelles[90].

La mise en œuvre de la CNIL intervient donc dans un objectif d'adaptation juridique au développement massif des nouvelles technologies de l'information et de la communication. En permettant une régulation en amont de l'entrée en vigueur des lois, cet organisme permet de prévenir certaines erreurs du législateur dans l'élaboration du cadre juridique de technologies numériques innovantes. Elle effectue une mise en balance entre sécurité et liberté par le biais de mise en ligne de débats faisant intervenir de multiples experts. La multiplicité des avis recueillis permet de rendre compte de nombreux défis et problématiques qu'engendrent l'explosion du numérique.

B) Un recul progressif des libertés individuelles

Les illustrations précédentes évoquent les dangers que représentent une trop grande assimilation des technologies numériques au sein des enquêtes judiciaires. En effet, l'exemple précédent démontre que la volonté du législateur est de développer massivement le recours aux techniques d'enquêtes numériques pour répondre aux exigences de réponse judiciaire à la délinquance. Un objectif qu'il tente d'atteindre au détriment des libertés individuelles.

L'effervescence juridique combinée à la refonte constante des règles juridiques encadrant les enquêtes judiciaires conduit le droit à reconnaitre de plus en plus de moyens empiétant sur les libertés individuelles. Le recours à l'IMSI catcher par exemple marque un pas en avant considérable vis-à-vis des écoutes judiciaires classiques. Ce système permet d'aller

[89] Contexte de l'urgence sanitaire en raison de la Covid-19
[90] Idem 74

jusqu'à l'interception de la contenance même des correspondances constituantes, par nature, une mesure particulièrement intrusive au regard de ces libertés. Ce dispositif dépasse de loin le cadre de écoutes téléphoniques plus classiques relevant, pour les enquêtes préliminaires et de flagrances et, des articles 706-95 du CPP.

Dans ce cadre, l'interception des correspondances émises par la voie des communications électroniques permet d'effectuer une écoute sur un appareil dont le numéro a déjà été identifié. A l'inverse, l'IMSI catcher permet d'intercepter toutes les données du trafic électronique qui entre dans son périmètre de recherche et ce, indépendamment de la connaissance préalable du numéro d'identification avec la possibilité de saisir l'ensemble qui lui sont associées. De surplus, il est possible de saisir l'ensemble des lignes qui lui sont associées. La frontière entre les écoutes classiques et de proximité a été franchis et acceptée par le Conseil constitutionnel ce qui représentent une menace grandissante pour la vie privée.

Le développement d'un autre outil numérique inquiète et pose de véritables problèmes d'atteinte à la vie privée : la reconnaissance faciale. Aujourd'hui, ces logiciels ont gagné en performance et fiabilité. Ils permettent de travailler avec des images de basse qualité incluant celles fournies par les caméras de vidéoprotection.

Son utilisation pose une problématique au regard des données personnelles et de leur sécurisation. En effet, l'utilisation que les dirigeants pourraient faire des données récoltées inquiètent les citoyens. Cette incertitude s'explique notamment par l'empiètement de plus en plus important sur les libertés telles que la vie privée ou la liberté d'aller et venir.

En 2012, le FBI avait investi un milliard de dollars dans un « programme d'identification de nouveau générateur » qui permettrait de constituer une base de données nationale photographique des criminels ainsi que quelques informations sur leurs données biométriques. A cette époque, la possibilité que les personnes au casier vierge et non suspectées puissent aussi figurer dans ce fichier et se retrouver surveillées, inquiétait les défenseurs des droits. Cette crainte semble désormais se justifier au regard des documents récupérés par la Fondation Electronic Frontier, une ONG à but non lucratif, selon lesquels 4,3 millions de clichés auraient été récupérés sans aucune enquête en cours ou implication criminelle[91].

[91] Murielle Cahen, « Les risques juridiques des logiciels de reconnaissance FACIALE », 2021, https://www.murielle-cahen.com/publications/reconnaissance%20-faciale.asp

On peut donc imaginer l'apparition de plusieurs situations : un innocent pourrait se retrouver au cœur d'une enquête criminelle, mais la technologie pourrait aussi être utilisée à mauvais escient dans le but d'atteindre d'autres objectifs visés par les pouvoirs politiques notamment pour réprimer l'opinion dissidente. La vulnérabilité que présentent les données numériques au piratage et aux utilisateurs malveillants suscitent de nombreuses inquiétudes.

Les dirigeants, œuvrant dans une optique de protection nationale, peuvent également s'en servir comme d'un moyen pour introduire de nouveaux dispositifs qui, dans un autre contexte, n'auraient eu aucune chance d'être adoptés.

De plus, les attentats terroristes survenus depuis 2015[92] ont rapidement fait progresser les techniques d'investigations numériques au sein des enquêtes, la gravité des crimes commis permettant de justifier leur mise en œuvre. En dehors de ce contexte particulier, ces dernières auraient probablement mis plus de temps à être acceptées dans la législation française. Les techniques spéciales d'enquêtes se sont développées de façon conséquente et une expérimentation des dispositifs de reconnaissance faciale a été mise en œuvre notamment à Paris.

Le même scénario s'est produit lors de l'apparition de la pandémie Covid-19 qui a atteint la population à l'échelle mondiale. Le contrôle de la propagation du virus puis du respect des confinements consécutifs par les citoyens français sont autant de raisons qui ont justifié l'expérimentation de dispositifs aéroportés. Ces derniers, extrêmement maniables ont la possibilité de se déplacer en hauteur et à distance et peuvent capter des images et sons à une distance tout aussi conséquente. Ces capacités, décuplées par les progrès technologiques, offrent des possibilités bien plus importantes qu'actuellement employées.

Enfin, malgré les multiples gardes fous protégeant les libertés individuelles, l'évolution de la société entraine inextricablement l'introduction de technologies modernes dans les moyens d'investigation. L'objectif primordial est d'adapter l'arsenal des forces de police aux enjeux de la délinquance moderne. Cependant, cela entrainera nécessairement une réduction des libertés individuelles comme c'est d'ores et déjà le cas : les techniques actuelles étant de plus en plus attentatoires.

[92] Attentats terroristes qui ont suivis ceux du 7 au 9 janvier 2015 visant Charlie Hebdo

§2 Différents modèles d'utilisation des technologies numériques en droit international

A) La Chine et la Russie : 2 régimes pour lesquels la sécurité Nationale prend le pas sur le respect de la vie privée

Simone Pieranni, aujourd'hui journaliste au sein du quotidien « China Files », a vécu en Chine entre 2006 et 2014. Dans son roman « *Red Mirror, L'avenir s'écrit en Chine* », il nous expose un regard éclairé sur la place du numérique en Chine.

A l'intérieur du pays, le numérique est bien plus développé qu'en France. Les chinois disposent d'une application appelée « WeChat » grâce à laquelle « on peut tout faire » selon le journaliste. En effet, elle permet à son utilisateur d'effectuer toutes les actions qu'il souhaite pendant sa journée. Il est non seulement possible de payer avec l'application la note d'un restaurant, de commander un taxi, trouver un bar à proximité, de passer commande, prendre des rendez-vous médicaux, consulter le magazine d'une enseigne mais aussi mille autres actions.

La plupart du temps, l'application fonctionne à l'aide de QR code qui sont omniprésents dans les villes chinoises. Cette « super application » est indispensable pour un citoyen chinois et, s'il ne la possède pas, c'est un véritable choix de vie. La personne qui décide de faire cela pour protéger ses données personnelles, que l'application collecte massivement, se retrouve à l'écart des autres citoyens. Une avocate ayant fait ce choix témoignait du handicap quotidien que cela lui procurait et, à l'évidence, elle se retrouvait dans la situation similaire à celle d'un français qui ne possèderait pas de téléphone.

En raison de cette omniprésence du numérique dans la vie des citoyens chinois, le gouvernement, lui aussi, s'est emparé des outils tels que l'intelligence artificielle et le Big Data pour lutter contre la délinquance mais, surtout, pouvoir contrôler la population.

Le dossier Xinjiang. Au nord Est de la Chine vit la minorité Ouïghour, un peuple turcophone musulman opprimé par le gouvernement chinois en raison de leur ethnie. En effet, ils se détachent de l'ethnie Han chinoise radicalement différente, qui est le groupe

majoritaire de la Chine. Dans cette région, le journaliste a constaté « la présence des points de contrôle sur les routes à la sortie des grandes villes et de la présence massive des policiers ». Il a été suivi pendant plusieurs jours par 2 fonctionnaires qui ont affirmé assurer sa sécurité. En effet, les ouïghours sont considérés comme des délinquants et, face à la menace Djihadiste grandissante, le gouvernement a amené la communauté internationale à reconnaitre la menace terroriste dans les Xinjiang. L'objectif officieux était d'essayer d'étouffer l'élan religieux de la région. Depuis quelques années, des Hans ont été envoyés pour surveiller massivement le Xinjiang et dans chaque quartier il existe désormais des postes de police, des milliers de caméras ont été installées et le territoire est parfois fermés vers l'extérieur.

Le programme « unis comme une seule famille ». Le pouvoir politique a mis en place une opération « éducative » pour laquelle au moins 1 million de chinois d'ethnie Han ont été déplacés au Xinjiang. Chaque fonctionnaire avait pour mission de devenir un parent d'une famille Xiang en s'installant chez elle et incarnant le rôle de « citoyen-policier ». Leur tâche consistait à surveiller la famille dont ils avaient la charge et leur apprendre la culture « patriotique » en langue mandarin et non Ouïghour avec une dévotion entière pour le président Xi Jinping. Ils sont aussi présents pour condamner et rapporter le comportement des familles sous surveillance. Ceux jugés négatifs conduisent les citoyens vers des camps de rééducation chinois.

Cet exemple démontre bien les limites et les dangers que représentent une utilisation des technologies numérique à des fins politiques. Ainsi, sous couvert de la protection de l'ordre public, le gouvernement porte de graves atteintes à la vie privée des citoyens. En effet, les avancées technologiques sont devenues un moyen d'opprimer des minorités ethniques en opposition avec l'ethnie du pouvoir politique. Cela démontre aussi l'importance de limiter les droits de l'Etat dans la mise en œuvre des dispositifs de surveillance pour garantir les libertés individuelles. En allant plus loin, à l'aide des multiples outils de surveillance le pouvoir politique pourrait étouffer toute opposition dissidente.

Crédit social. Le système de « crédit social » est un autre exemple de détournement des technologies numériques qui peut exister. C'est un mécanisme inventé par les pouvoirs publics chinois pour tenter de parer aux difficultés liées à l'application des lois et règlements. Il s'agit d'un système de collecte des données de chaque individu basé sur le Big Data. Leurs casiers judiciaires, leurs historiques de paiement, leurs incivilités sont autant d'informations

analysées dans le but d'attribuer un nombre de points. Pour ce faire, des milliers de caméras dotées de logiciels de reconnaissance faciale ont été installées permettant un système de surveillance à grande échelle. En fonction de ce score, les citoyens pourront soit accéder à des privilèges, tels que le droit d'inscrire ses enfants dans une école réputée ou bien avoir moins de temps d'attente pour accéder à des services publics, soit avoir un malus qui aura un impact sur la possibilité d'obtenir un prêt par exemple. Ce sont des algorithmes qui permettent d'établir ce score à partir des données récoltées.

De plus, au sein de la ville de Shenzhen sont affichés aux coins des carrefours de grands panneaux qui analysent les visages des passants. La mégalopole de Shanghaï inflige des contraventions aux personnes qui commettent une « infraction » en traversant au feu rouge, leur visage est ensuite affiché sur les écrans des arrêts de bus du quartier grâce à une capture via reconnaissance faciale. Ainsi, les dirigeants ont inventé une autre forme de sanction pour assurer le respect des règles de « bienséance » en affichant publiquement les visages, révélant leurs identités, pour les présenter comme des délinquants.

C'est une forme de contrôle de la population très attentatoire au respect de la vie privée ainsi qu'à la liberté d'aller et venir. Elle réduit la vie sociale des citoyens à une note basée sur la scrutation de leurs faits et gestes, bonnes et mauvaises actions dont l'évaluation est laissée à la libre appréciation du gouvernement.

Ces exemples nous exposent un tableau représentant les plus grandes inquiétudes de notre ère concrétisées à l'heure actuelle. Ainsi, à l'image d'un épisode de la série Black Mirror, dans lequel le monde est policé, chaque geste est soumis à l'appréciation générale et jaugé sans pitié, l'exemple de la Chine est une fiction devenue réalité. Dans cet épisode, un système de notation détermine le statut social de chaque personne ce qui lui permet d'accéder à divers avantages tels que l'octroi d'un prêt bancaire ou encore l'accès à certains évènements prestigieux. Une note de 0 à 5 est attribuée à chaque personne et, si la note est trop basse, l'individu deviendra un paria, il sera exclu de la société.

B) Les EU : Les forces de police disposant d'une grande autonomie dans les enquêtes judiciaires

Arno Amabile et Basile Thodoroff ont coécrit un ouvrage intitulé « *Police numérique, une révolution sous surveillance ?* » qui décrit comment les Etats-Unis ont assimilé le phénomène du Big Data ainsi que de l'intelligence artificielle au sein des enquêtes judiciaires.

La particularité du modèle politique américain réside dans son fédéralisme. De cette manière, la gestion des forces de police relève de la responsabilité des villes, contés et parfois des états. Ceux-ci disposent d'une grande autonomie en ce qui concerne leur organisation et leurs équipements. La volonté des pouvoirs publics de pouvoir prédire où et quand les crimes seraient susceptibles d'avoir lieu a conduit à l'apparition du phénomène dit « predictive policing »[93]. Un mouvement de réformes aux Etats-Unis a ensuite souhaité rendre la police plus proactive et vigilante, réactive et urgentiste qu'auparavant. La volonté était de rendre les forces de polices plus avancées dans la production de sécurité que dans la répression.

A partir de la fin des années 1990, les technologies du big data et des analyses prédictives ont ainsi fait évoluer les techniques de maintien de la sécurité publique mais aussi de gestion des forces de police aux Etats-Unis. C'est seulement après 2007 qu'ont commencé à se développer les méthodes de « police prédictive », commercialisées par les sociétés telles que PredPol, Palantir et Hunchlab. Initialement, ces outils devaient permettre de faire face aux cas de criminalité graves, dans un contexte de violence urbaine armée, certains états autorisant le port d'armes. Pour mettre un terme à cette violence, des outils de police prédictive ont été déployés dans plusieurs villes.

Prenons l'exemple de « PredPol ». C'est un logiciel de prédiction des délits employé dans plusieurs villes telles que Atlanta et Palo-Alto qui permet de prédire les zones géographiques à risque.

Predpol a permis de changer la nature de l'interaction entre la police et la machine. En effet, il va désigner des quartiers de villes dans lesquels les crimes et délits seraient susceptibles de se produire en utilisant les bases de données historiques des crimes ainsi que les données démographiques et géographiques locales. Cela lui permet d'estimer les probabilités d'apparition d'un crime sur des zones de 50m² et de prévoir l'infraction sur une période

[93] Police prédictive

pouvant aller jusqu'à 28 jours[94]. L'objectif est d'aider les enquêteurs à orienter ses interventions. La plateforme fournit des cartes simplifiées qui indiquent les risques par la présence d'un carré rouge sur une carte. Les prédictions sont alors projetées sur un plan dans l'objectif de déclencher une action de la police. Des doutes ont été émis sur son efficacité mais ils n'ont pas été suffisants pour arrêter son adoption.

Selon Céline Castets-Renard, le développement de ces outils de police prédictive s'explique aussi par la crise de confiance envers la police qui est apparue ces dernières années. Les violences policières, qui atteignaient particulièrement les afro-américains, ont conduit à la rechercher des moyens plus objectifs pour faire face aux accusations racistes portées notamment par le mouvement « Black Lives Matter »[95].

Les logiciels de prédiction des crimes ne sont pas les seuls outils numériques à intégrer les méthodes d'investigation des forces de police. En 2017, 347 forces de police municipales ou étatiques ont emboité le pas à Los Angeles en s'équipant de drones selon les auteurs[96]. Ce sont des technologies beaucoup plus développées que ce que nous connaissons actuellement en France et qui ne pourraient être admises aussi aisément.

Leur utilisation pose cependant des enjeux juridiques importants. Ces outils de police prédictive peuvent devenir rapidement attentatoires aux droits et libertés fondamentaux des personnes si aucune précaution juridique n'est prise en amont. Cependant, les risques les plus graves sont encourus non pas lorsque les logiciels ciblent des lieux mais des personnes. En effet, il existe des risques de réidentification et le traitement massif de données personnelles employé par ces programmes peuvent rapidement engendrer des débordements.

Ces constatations sont exacerbées par le fait qu'aux Etats Unis, les citoyens ne bénéficient pas d'une protection aussi développée qu'en France. De cette manière, le Pryvacy Act[97] couvre uniquement l'emploi de ces outils « par les seules agences fédérales traitant des données portant sur des personnes identifiables et incluses dans une base de données, ce qui

---

[94] Arthur Le Denn, « La police de Los Angeles abandonne PredPol, le logiciel qui prédit les crimes », 2020, https://www.usine-digitale.fr/article/la-police-de-los-angeles-abandonne-predpol-le-logiciel-qui-predit-les-crimes.N956926

[95] Céline Castets-Renard, « L'IA en pratique : la police prédictive aux États-Unis », Dalloz IP/IT, 2019, https://www-dalloz-fr.lama.univ-amu.fr/documentation/Document?ctxt=0_YSR0MD1wb2xpY2UgcHLDqWRpY3RpdmUgw6l0YXRzIHVuaXPCp3gkc2Y9c2ltcGxlLXNlYXJjaA%3D%3D&ctxtl=0_cyRwYWdlTnVtPTHCp3MkdHJpZGF0ZT1GYWxzZcKncyRzb3J0PSNkZWZhdWx0X0Rlc2PCp3Mkc2xOYlBhZz0yMMKncyRpc2Fibz1UcnVlwqdzJHBhZ2luZz1UcnVlwqdzJG9uZ2xldD3Cp3MkZnJlZXNjb3BlPUZhbHNlwqdzJHdvSVM9RmFsc2XCp3Mkd29TUENIPUZhbHNlwqdzJGZsb3dNb2RlPUZhbHNlwqdzJGJxPcKncyRzZWFyY2hMYWJlbD3Cp3Mkc2VhcmNoQ2xhc3M9&id=DIPIT%2FCHRON%2F2019%2F0234

[96] Basile, Thodoroff, Arno Amabile, « Police numérique, une révolution sous surveillance ? États-Unis et Chine, 2 modèles repoussoirs », Ecole des Mines, 2020

[97] Loi sur la protection de la vie privée

exclut les traitements par les acteurs privés, ainsi que par les agences étatiques et municipales »[98]. Cet exemple démontre la présence de lacunes législatives laissant la porte ouverte à la mise en péril et au recul progressif des droits et libertés fondamentaux si aucun encadrement n'est envisagé.

L'existence de biais et discriminations des outils de police prédictive ont aussi alerté sur l'atteinte au principe d'égalité garantissant une égale protection des citoyens devant la loi.

Enfin, la garantie d'un procès régulier par ces outils a aussi été discutée. Le logiciel Palantir Gotham employé à New York a dû préciser en justice ses modalités d'utilisation. En effet, « le manque d'informations sur l'existence et l'utilisation de l'outil prédictif, ainsi que sur la nature des données concernées et les conditions de mise en œuvre des résultats algorithmiques du traitement automatisé ont été contestés sur le fondement d'un défaut de transparence et de l'impossibilité de faire respecter les droits de la défense »[99].

Finalement, l'emploi de ces outils numériques en France connait de nombreux défis d'encadrement juridique qui tendent à être corrigés par l'intervention du législateur sous le contrôle effectif du Conseil constitutionnel. Les risques engendrés pour les libertés individuelles, par l'utilisation massive de ces outils qui se sont illustrés à l'international, et les failles algorithmique, résultant de l'intervention humaine dans leur conception, sont autant d'obstacles à son développement en France.

Mais les services judiciaires ne sont désormais plus les seuls à exploiter les avancées numériques, les citoyens, avec leurs propres moyens, œuvrent parallèlement aux enquêteurs.

[98] Idem 83
[99] Idem 83

Partie 2_ L'emploi de nouvelles technologies par les citoyens s'affranchissant du droit

Certains citoyens ont décidé d'œuvrer à leur échelle pour lutter contre la criminalité. Ils disposent de moyens d'enquêtes numériques bien plus étendus que les services judiciaires en raison d'un cadre juridique peu rigoureux et dont les contours tardent à être définis (chapitre 1). C'est cependant pour cette raison que cette « justice citoyenne » engendre de nombreux défis qui questionnent sur la place qu'ils pourront occuper (chapitre 2).

Chap 1 Les citoyens disposant de moyens d'enquêtes numériques plus étendus

Cette lutte se matérialise de différentes manières, par des rassemblements citoyens ou bien par l'œuvre isolée de certains individus. Ainsi, ces enquêtes sont menées à la fois en open source par des sociétés privées (section 1) mais aussi par des citoyens qui disposent de moyens d'enquêtes plus étendus en raison de l'absence de cadre juridique (section 2).

Section 1) Des capacités d'enquêtes décuplées par l'open source mises à profit par les sociétés privées

Les sociétés de journalisme réalisent désormais des investigations en exploitant les ressources qu'offrent l'Open Source (§1) qui, par leur innovation, engendrent de nombreux enjeux à l'échelle mondiale (§2).

§1 L'exploitation des données accessibles en source ouverte

Si l'Etat a vu par le développement du numérique une opportunité pour améliorer les techniques d'enquêtes judiciaires, c'est aussi le cas des sociétés privées et notamment des journalistes. Albane Dreyer, journaliste diplômée de CELSA[100], souligne dans son article intitulé « L'investigation numérique, révolution de la pratique journalistique » que le terrain, qui était auparavant le principal lieu pour enquêter, est aujourd'hui relayé au second plan car le digital a pris sa place. Cette révolution du numérique a donc atteint les moyens utilisés par les reporteurs et on parle désormais de « journalisme en sources ouvertes ».

Cette appellation est tirée de l'expression Open Source qui signifie source ouverte. A l'origine cela faisait référence aux logiciels Open Source. C'est une « *méthode d'ingénierie logicielle qui consiste à développer un logiciel, ou des composants logiciels, et de laisser en libre accès le code source produit* »[101]. Plus précisément, certaines œuvres, en dehors de celles tombées dans le domaine public, sont libres par la volonté de leur auteur. L'objectif est de faciliter la diffusion et le partage d'idées. Cependant, chaque logiciel possède initialement un auteur déterminé lors de sa création qui, de ce fait, est investi de droit moraux et patrimoniaux[102]. Pour les seconds, il est possible d'y renoncer de façon expresse alors que pour les premiers, cela est interdit par la loi française.

En revanche, l'auteur peut toujours divulguer son droit de façon anonyme pour contourner cette interdiction et ainsi pouvoir le partager. Un logiciel est alors libre lorsque sa « source est ouverte », que l'on va qualifier d'open source, ce qui va permettre à chaque internaute de l'obtenir et de modifier son code source. Ainsi, il pourra être adapté en fonction des besoins de son utilisation et redistribué.

Ces logiciels sont développés par une communauté de manière collaborative puis rendus publics. De cette façon, chaque utilisateur pourra, en tant que coopérateur occasionnel, coopérer à son perfectionnement et permettre sa mise à jour régulière de sorte qu'il soit

[100] Ecole des hautes études en sciences de l'information et de la communication interne à Sorbonne Université.
[101] Cyrille Chausson, Définition Open Source, 2016, https://www.lemagit.fr/definition/Open-Source
[102] Philippe le Tourneau, , « Chapitre 221 - Qualification du logiciel », *Dalloz référence Contrats du numérique*, Dalloz, 2021-2022, https://www-dalloz-fr.lama.univ-amu.fr/documentation/Document?id=DZ%2FREFERENCE%2FCONTRATS-NUMERIQUE%2F2020%2FL02-T22-C221%2FPLAN%2F0002&ctxt=0_YSR0MD1vcGVuIHNvdXJjZSBpbnRlbGxpZ2VuY2XCp3gkc2Y9c2ltcGxlLXNlYXJjaA%3D%3D&ctxtl=0_cyRwYWdlTnVtPTHCp3MkdHJpZGF0ZT1GYWxzZcKncyRzb3J0PSNkZWZhdWx0X0Rlc2PCp3Mkc2xOYlBhZz0yMMKncyRpc2Fibz1UcnVlwqdzJHBhZ2luZz1UcnVlwqdzJG9uZ2xldD3Cp3MkZnJlZXNjb3BlPUZhbHNlwqdzJHdvSVM9RmFsc2XCp3Mkd29TUENIPUZhbHNlwqdzJGZsb3dNb2RlPUZhbHNlwqdzJGJxPcKncyRzZWFyY2hMYWJlbD3Cp3Mkc2VhcmNoQ2xhc3M9&scrll=DZ%2FREFERENCE%2FCONTRATS-NUMERIQUE%2F2020%2FPARA%2F221.21

toujours en phase avec l'actualité. Une erreur dans le programme ou un mauvais fonctionnement sera amélioré très rapidement.

Le développement concomitant d'Internet a permis de faciliter grandement l'échange des informations et des nouvelles versions des logiciels ouverts. C'est dans ce contexte que le journalisme numérique s'est développé, leurs méthodes d'investigations se basant sur l'exploitation de logiciels ouverts dont les données sont librement accessibles.

Cette méthode a été élaborée par Eliot Higgins au début des années 2010 lorsqu'il a traqué les armes utilisées dans le conflit syrien en se basant sur des milliers de photos et de vidéos publiées sur le Internet. Après cela, il a créé Bellingcat, un site d'information spécialisées dans l'Open Source Intelligente, qui a trouvé une démonstration pratique lorsqu'il a permis de prouver, en 2014, la responsabilité de l'armée russe dans le tir de missile qui a abattu le vol MH17 de Malaysian Airlines au-dessus de l'Ukraine.

Le Big Data est donc au cœur des enquêtes journalistiques mais, avant tout développement, il est important de définir le « data journalisme » et ses enjeux. Chaque action réalisée sur un réseau social laisse différentes traces et ces données vont être trouvées et analysées par les « data journalistes » pour révéler les évènements importants et déchiffrer l'actualité. Cela va à la fois permettre de déterminer quelles sont les actions qui influent sur les évènements en question mais aussi une meilleure transmission des informations. La technique d'exploitation des sources d'informations en libre accès tels que les journaux et les sites web est appelée Open Source Intelligente (OSINT).

L'affaire de Skripal est une illustration de l'apport indiscutable que peut permettre les enquêtes en open source. De cette manière le travail du site intitulé « BellingCat » a permis d'identifier les personnes responsables d'un empoisonnement seulement à l'aide des données disponibles en source ouverte. En l'espèce, le 4 mars 2018 en Grande Bretagne, Sergueï Skripal, ancien agent double russe, et sa fille sont empoisonnés au Novichok : un gaz innervant soviétique. Les autorités britanniques avaient, à l'aide de caméras de vidéosurveillance identifié deux hommes suspects. Ils étaient ensuite apparus à la télévision pour tenter de se disculper. Cependant, les nomes qu'ils avaient donné étaient des faux et les autorités soupçonnaient les individus de faire partie des agents de service des renseignements militaires russes.

Le site BellingCat est donc spécialisé dans la recherche d'informations disponibles sur internet et les réseaux sociaux. Le G29, comité consultatif des autorités nationales des États membres de l'Union européenne en charge de la protection des données à caractère personnel, définit les services de réseaux sociaux comme « des plateformes de communication en ligne qui permettent à tout internaute de rejoindre ou de créer des réseaux d'utilisateurs ayant des options similaires et/ou des intérêts communs ».

La particularité du site est que, pour chaque investigation menée, il dévoile ses méthodes de recherches. Dans cette affaire, il explique avoir recherché sur l'Internet russe des photos des hommes suspectés. Ils ont ensuite ciblé les promotions des académies militaires[103] où les agents auraient pu étudier. Cette technique leur a permis de dévoiler les identités réelles des deux hommes.

Les données récoltées par les journalistes sont produites par les utilisateurs d'Internet et peut provenir de diverses sources telles que des post photos ou vidéos sur Instagram, Facebook ou bien encore la géolocalisation de ces publications. Ce fut le cas lors des violences qui ont eu lieu au Capitol américain en 2021 lorsque des manifestants pro-Trump attaquaient le Capitole. De nombreuses vidéos ont été publiées sur les réseaux par des touristes et partisans de Donald Trump qui ont permis de découvrir comment l'entrée du Capitole avait été forcée. De plus, à l'aide d'un logiciel de reconnaissance faciale, le « Washington Post » a pu identifier certains responsables[104].

Une autre affaire révèle les capacités des investigations menées uniquement en open source que possèdent les data journalistes. En juillet 2018, une vidéo est diffusée sur les réseaux sociaux, laquelle montre deux femmes et deux enfants qui sont emmenées par des hommes armés sur un chemin de terre et exécutées. En revanche, aucun détail concernant le lieu et la date à laquelle cet évènement a eu lieu. C'est le travail de la BBC Eye Africa qui est une unité d'enquête spécialisée sur l'Afrique de la BBC, qui a résolu l'affaire. En effet, en utilisant à la fois des sources ouvertes en ligne et des techniques classique des journalistes,

[103] Simon Petite, « Bellingcat, le site qui aligne les révélations sur l'affaire Skripal », 2018 https://www.letemps.ch/monde/bellingcat-site-aligne-revelations-laffaire-skripal

[104] Albane Dreyer, « L'investigation numérique, révolution de la pratique journalistique », 2021 https://www.mesdatasetmoi-observatoire.fr/article/linvestigation-numerique-revolution-de-la-pratique-journalistique

la BBC a découvert le lieu exact des meurtres, la date à laquelle ils ont été perpétrés ainsi que l'identité des auteurs[105].

Le succès retentissant qui a résulté de la résolution de cette affaire a prouvé l'efficacité que pouvait revêtir les investigations menées par une collaboration entre une société privée de journalisme et des internautes indépendants. Cela représente une avancée de taille dans la lutte contre la délinquance notamment marquée par l'absence totale des services d'enquête judiciaire de l'Etat. En effet, cela signifie que la résolution de l'affaire résulte uniquement de l'exploitation des données en sources ouvertes c'est à dire accessibles aux internautes sans habilitation quelconque.

En dépit de la réussite notable de ces nouvelles techniques d'enquêtes, l'utilisation de l'open source possède toutefois des limites. Malgré ses nombreuses sources, la BBC News n'a pas pu découvrir l'identité des quatre victimes. Pour continuer l'enquête, les journalistes auraient désiré se rendre sur les lieux mais c'est une zone qualifiée de « trop dangereuse[106] » et cela s'est donc révélé infaisable.

A ce titre Google Earth est un outil de l'open source intelligence qui recèle de nombreuses données exploitables dans le cadre d'enquêtes journalistiques. Son usage a notamment permis d'établir avec certitude que les forces de l'ordre Iraniennes ont effectivement tiré de façon répétée sur des individus manifestants contre la hausse des prix de l'essence en novembre 2019. L'équipe des Observateurs de France 24 a pu en attester après avoir analysé plus de 750 photographies et vidéos amateurs avec des outils comme SunCalc et Google Earth. Tout cela est réalisé à distance sans que les équipes de journalistes se soient rendus sur place.

En l'espèce, entre le 15 et le 18 novembre 2019, lors de ces manifestations, des centaines de personnes ont été tuées en Iran. Cette répression a été menée par les forces de l'ordre iraniennes qui ont veillé à assurer un huit clos. C'est dans ce contexte que les accès Internet et aux télécommunications ont été coupées par le gouvernement. Ce n'est que lors du rétablissement des connexions qu'une multitude de vidéos ont été publiés sur le web et les réseaux sociaux. On peut observer des policiers abattre et blesser par arme à feu des

[105] Faustine Vincent, « Comment la BBC a retrouvé le lieu et la date d'exécutions filmées au Cameroun », 2018, https://www.lemonde.fr/big-browser/article/2018/09/27/executions-filmees-au-cameroun-la-prouesse-journalistique-de-la-bbc_5360895_4832693.html
[106] Idem

manifestants non armés. Les observateurs de France 24 ont exploité les photos et vidéos enregistrés par des témoins exposant les tirs et blessures dans le chaos ambiant.

En utilisant des techniques de géolocalisation couplées avec des informations fournies par les internautes qui avaient publié les vidéos, ils ont pu déterminer la localisation exacte d'une trentaine de vidéos, montrant des hommes en uniforme faire feu sur des civils[107].

Ces nombreuses enquêtes menées par les sociétés de journalisme poursuivent un objectif de lutte contre la désinformation, révélant la vérité sur des crimes commis et étouffés par les autorités politiques de pays peu respectueux des droits et libertés fondamentaux.

C'est aussi en utilisant Google Earth que le média français d'investigation Disclose a pu prouver en 2019 que des armes françaises étaient bel et bien utilisées dans le conflit yéménite, contrairement aux déclarations répétées de la ministre des armées Florence Parly. C'est en repérant, à l'aide d'images satellites à des dates précises, l'apparition de camions français "Caesar" sur des images satellites au port de Jeddah, en Arabie Saoudite, et en identifiant ces mêmes camions aux alentours des villages visés par des attaques militaires au Yémen, qu'ils ont pu rétablir la vérité.

Enfin, pour recourir à l'Open Source Intelligence il est nécessaire de connaitre plusieurs méthodes de recherche sur Internet. Des notions essentielles en lien avec les cybermenaces et la protection du Web devront être maitrisées par les journalistes.

§2 Les enjeux des investigations par l'Open Source Intelligente

Manipulation de l'information. Les ressources disponibles en source ouverte sur les réseaux sociaux et Internet présentent une multiplicité et une diversité de données qui permet aux sociétés journalistiques d'enquêter de façon approfondie sur les sujets envisagés. Cependant, ce sont autant de possibilités de découvrir des fausses informations, erreurs ou encore des fausses pistes. Un enjeu non négligeable apparait alors, c'est la détection des « fake news ». En anglais, fake signifie « faux », il s'agit donc de fausses informations

[107] Les Observateurs, « Les observateurs France 24, Enquête vidéo : Iran, massacre à huis clos », 2020, https://observers.france24.com/fr/20200110-enquete-video-iran-massacre-manifestations-internet

générées par les internautes mais surtout d'informations délibérément fausses dont la diffusion vise à induire en erreur.

C'est une stratégie de désinformation[108] qui a fait l'objet de nombreuses publications des médias notamment lors des élections présidentielles. Aux Etats-Unis comme en France, Donald Trump et Emmanuel Macron se sont retrouvé être les sujets de fausses informations diffusées dans le but de mettre à mal leurs campagnes électorales.

Pour lutter contre ce phénomène, ont été promulguées les lois organiques du 22 décembre 2018 relatives à la lutte contre la manipulation de l'information. Elles permettent, dans une période de 3 mois précédant un scrutin de saisir le tribunal de grande instance de Paris en référé pour qu'il ordonne de mettre fin à la diffusion d'« allégations ou imputations inexactes ou trompeuses d'un fait de nature à altérer la sincérité du scrutin »[109].

Plus précisément, cette action vise spécifiquement les fakes news « diffusées de manière délibérée, artificielle ou automatisée et massive par le biais d'un service de communication au public en ligne » et peut être initiée « à la demande du ministère public, de tout candidat, de tout parti ou groupement politique ou de toute personne ayant intérêt à agir »[110].

Si la loi protège les candidats en période électorale, c'est aussi le cas en dehors de ce contexte particulier. De cette manière, il est prévu que les opérateurs de plateforme mettent en place « un dispositif facilement accessible et visible permettant à leurs utilisateurs de signaler » les fausses informations, « notamment lorsque celles-ci sont issues de contenus promus pour le compte d'un tiers ».

En outre, ces opérateurs sont également tenus de mettre en œuvre les mesures complémentaires dans certains domaines afin de lutter contre la diffusion de fausses informations : « 1° La transparence de leurs algorithmes; 2° La promotion des contenus issus d'entreprises et d'agences de presse et de services de communication audiovisuelle; 3° La lutte contre les comptes propageant massivement de fausses informations; 4° L'information des utilisateurs sur l'identité de la personne physique ou la raison sociale, le siège social et l'objet social des personnes morales leur versant des rémunérations en contrepartie de la

[108] Christiane Féral-Schuhl, , « Chapitre 712 - Atteintes aux systèmes d'information », *Praxis Cyberdroit*, 2020-2021, https://www-dalloz-fr.lama.univ-amu.fr/documentation/Document?id=DZ%2FPRAXIS%2FCYBERDROIT%2F2019%2FL07-T71-C712%2FPLAN%2F0010&ctxt=0_YSR0MD1mYWtlIG5ld3PCp3gkc2Y9c2ltcGxlLXNlYXJjaA%3D%3D&ctxtl=0_cyRwYWdlTnVtPTHCp3MkdHJpZGF0ZT1GYWxzZcKncyRzb3J0PSNkZWZhdWx0X0Rlc2PCp3Mkc2xOYlBhZz0yMMKncyRpc2Fibz1UcnVlwqdzJHBhZ2luZz1UcnVlwqdzJG9uZ2xldD3Cp3MkZnJlZXNjb3BlPUZhbHNlwqdzJHdvSVM9RmFsc2XCp3Mkd29TUENIPUZhbHNlwqdzJGZsb3dNb2RlPUZhbHNlwqdzJGJxPcKncyRzZWFyY2hMYWJlbD3Cp3Mkc2VhcmNoQ2xhc3M9&scrll=DZ%2FPRAXIS%2FCYBERDROIT%2F2019%2FPARA%2F712.101

[109] Article L. 163-2 du Code électoral

[110] Idem 97

promotion de contenus d'information se rattachant à un débat d'intérêt général; 5° L'information des utilisateurs sur la nature, l'origine et les modalités de diffusion des contenus; 6° L'éducation aux médias et à l'information ».

Bien entendu, malgré la volonté des autorités publiques de prévenir l'apparition de fake news, ces dernières sont partagées encore plus vite que les informations pertinentes. Partant de cet état de fait, les sociétés privées de journalismes connaissent aujourd'hui une charge de travail multipliée par ce phénomène. La recherche de l'origine de l'information, sa confrontation avec la réalité ainsi que les preuves de son authenticité sont autant d'étapes supplémentaires à la conduite des investigations en Open Source. Il n'existe d'ailleurs pas seulement de fausses informations mais aussi des informations vraies dont la date a été modifiée et qui peut remonter à des dizaines d'années en arrière.

Le journaliste devra donc effectuer un double travail d'enquête, recherchant à la foi des informations d'actualité authentiques et, le cas échéant, devra établir le lieu, la date exacte ainsi que le contexte et l'identité des protagonistes. Ces étapes sont devenues nécessaires pour la publication d'articles fiables dont la pertinence et l'authenticité influent sur la réputation du journal à l'origine de ce dernier.

L'enjeu de l'Open Source Intelligence est donc de permettre un regroupement, une analyse minutieuse des données ainsi que de disposer de données non-biaisées.

Objectif de transparence. Le travail des journalistes est également d'offrir une transparence totale vis-à-vis des internautes. En effet, il ne suffit pas de démontrer, il est aujourd'hui nécessaire d'expliquer la démarche suivie.

Un article publié par Le Monde, le 27 septembre 2018 intitulé « Comment la BBC a retrouvé le lieu et la date d'exécutions filmées au Cameroun » nous apprend de quelle manière l'enquête a été menée. D'après la chronique, les journalistes se sont servis de la « forme des montagnes, végétation, bâtiments, position du soleil, couleur des treillis… » pour mener leurs investigations. Ils ont recouru aux technologies numériques pour analyser les différents éléments recueillis ainsi qu'au croisement des informations avec d'autres provenant de diverses sources telles que les réseaux sociaux ou encore des sources directes.

Par soucis de transparence, la BBC news a, de la même manière que BellingCat, partagé publiquement ses investigations. Elle a dévoilé, dans une vidéo nommée « Anatomy of a Killing[111] », de façon détaillée toute leur enquête et les méthodes utilisées. La première étape fut de localiser la vidéo. Pour cela, les journalistes ont recherché sur Google Earth à quelle montagne correspondait la crête aperçue sur la vidéo. Cet outil permet d'accéder à des images satellite, des reliefs, des cartes ou des bâtiments 3D de n'importe quel lieu dans le monde. Mais le plus intéressant est qu'il conserve ses archives en ligne. Il est donc possible d'observer des modifications d'une année à l'autre.

D'autres internautes analysaient la topographie des lieux de façon indépendante et les journalistes de la BBC ont décidé de s'associer à eux en créant un groupe Twitter pour mettre leurs mettre leur travail en commun. Un membre d'Amnesty International faisait aussi partie des recherches. C'est une source extérieure qui les a orientés vers le nord de lu Cameroun et leur a permis de trouver la localisation exacte en seulement quelques minutes.

La deuxième étape de leur enquête constituait à établir la date à laquelle la vidéo avait été tournée. Les enquêteurs ont alors eu recours à l'entreprise DigitalGlobe, qui permet par des images satellites datées d'observer l'apparition de bâtiments au fur et à mesure du temps. Effectivement, en recoupant les bâtiments visibles sur la vidéo et l'outil numérique les journalistes ont pu établir que les meurtres avaient eu lieu entre novembre 2014 et février 2016. Puis, un chemin de terre qui n'apparait qu'en période sèche lorsqu'on observe les images satellites réduit encore la période. Finalement, c'est l'un des internautes qui, en proposant une formule mathématique pour calculer la position du soleil à partir de l'ombre d'un des soldats, parvient à établir que le crime a eu lieu entre le 20 mars et le 5 avril 2015[112].

Enfin, concernant l'identité des auteurs, le gouvernement camerounais qui, au départ, avait nié l'implication des militaires dans le crime, a publié la liste de sept militaires qui ont fait l'objet d'une arrestation et d'une enquête. Si bien que, en croisant ces noms avec ceux mentionnés dans la vidéo et les profils Facebook, plusieurs auteurs ont été formellement identifiés.

[111] BBC News, Anatomy of a Killing, 2018, https://www.youtube.com/watch?v=4G9S-eoLgX4
[112] Faustine Vincent, « Comment la BBC a retrouvé le lieu et la date d'exécutions filmées au Cameroun », 2018, https://www.lemonde.fr/big-browser/article/2018/09/27/executions-filmees-au-cameroun-la-prouesse-journalistique-de-la-bbc_5360895_4832693.html

Le cas de l'Ukraine. L'open Source Intelligente s'est révélée receler plus de ressources que son utilisation initiale dans la résolution d'enquêtes : son exploitation a été déterminante dans la guerre en Ukraine. Le 24 février 2022, le président russe Vladimir Poutine a annoncé le début d'une opération de « pacification » et de « dénazification » de son pays frontalier, l'Ukraine. 150 000 soldats avaient déjà été postés à la frontière entre les deux pays mais c'est cette annonce qui a entrainé l'invasion de ces milliers de militaires armés en Ukraine. Début mars, le procureur général de la Cour pénale internationale (CPI) a ouvert une enquête sur les crimes commis en Ukraine. Fin avril, la procureure générale d'Ukraine, Iryna Venediktova, a indiqué qu'ont été recensé plus de 8.000 cas présumés de crimes de guerre.

Un long travail d'investigation a débuté pour les enquêteurs pour obtenir des preuves irréfutables et ainsi permettre de qualifier juridiquement les crimes commis pour pouvoir engager les poursuites contre les auteurs et leurs commanditaires.

C'est au cœur de ce conflit que les réseaux sociaux se sont démontrés être une arme redoutable permettant aux forces militaires de Volodymyr Zelensky, président de l'Ukraine, de préserver un avantage stratégique sur les opérations ennemies[113].

Les conflits armés récents se trouve désormais inextricablement liés à la connectivité globale. Peu après le début de l'invasion, Elon Musk a mis en place le déploiement du réseau dénommé Starlink en Ukraine. Celui-ci permet aux soldats ainsi qu'aux habitants du pays d'avoir accès à Internet malgré la destruction de plusieurs infrastructures par les missiles et les troupes russes. Indispensable pour permettre le partage de données, il a eu de nombreuses conséquences positives pour les Ukrainiens.

Parmi les différents réseaux sociaux, Twitter est devenu, dans ce contexte, une véritable base de renseignements. Quelques jours après le début du conflit, de nombreuses vidéos et photographies sont publiées sur ce réseau dévoilant à la fois des positions militaires mais aussi du matériel russe. Ces renseignements ont permis aux forces ukrainiennes de prévoir des mouvements russes, d'organiser une défense et même de préparer des contre-offensives. Le recueil et l'exploitation des données partagées a donc été stratégiquement

[113] Dorian De Schaepmeester, « Comment l'open source intelligence est devenue une arme majeure dans la guerre en Ukraine ? », 2022, https://www.futura-sciences.com/tech/actualites/guerre-futur-crimes-guerre-ukraine-ces-francais-traquent-preuves-98366/

décisive entrainant une nouvelle stratégie : le gouvernement ukrainien a spécifiquement demandé à certains journalistes de ne pas révéler de documents permettant de situer géographiquement les troupes du pays.

Par exemple la position de soldats russes été dévoilée par l'application Tinder, les soldats russes communiquant avec des femmes ukrainiennes par le biais l'application, alors que celle-ci fonctionne à partir d'un système de géolocalisation.

Enfin, l'OSINT permet d'analyser les conflits à distance. De cette manière les analystes ont pu découvrir l'emploi de missiles à sous munition en Ukraine alors que ces armes sont prohibées depuis un traité signé en 2008[114].

La démarche utilisée par les sociétés de journalisme d'OSINT est désormais bien établie. Preuve de cet état de fait, en 2015, la Cour pénal international a émis un mandat d'arrêt basé uniquement sur des preuves vidéo provenant de médias sociaux. C'est une première qui ne va pas s'arrêter là puisque dorénavant, les ONG se servent aussi de l'OSINT et incitent les citoyens à faire de même pour prouver des atteintes aux droit fondamentaux.

En France, l'association Open Facto propose une méthodologie permettant de mettre la lumière les violations des embargos sur les armes partout dans le monde. OpenFacto, qui est l'équivalent français de Bellingcat, est un journal qui effectue actuellement un travail d'enquête sur la guerre en Ukraine en exploitant les informations obtenues sur les réseaux sociaux. Ils basent leurs recherches sur 2 axes particuliers : ils collaborent avec des organisations qui ont structuré la collecte et la recherche d'informations notamment avec le Center for Information Resilience. Une deuxième collaboration out aussi importante est leur travail avec des juristes spécialisés dans ce domaine[115]. Cette dernière est primordiale puisqu'une vidéo ne peut pas faire lieu de preuve si elle n'est pas contextualisée de manière à avoir une valeur juridique.

[114] Convention sur les armes à sous-munitions

[115] Marc Zaffagni, « Crimes de guerre en Ukraine : ces Français traquent les preuves », 2022, https://www.futura-sciences.com/tech/actualites/guerre-futur-crimes-guerre-ukraine-ces-francais-traquent-preuves-98366/

Finalement, les réseaux sociaux concentrent désormais une base de centralisation des actualités du monde entier, permettant à la fois d'enquêter sur des infractions commises à l'étranger et à distance mais aussi sur des conflits armés en cours. L'enjeu de l'exploitation de l'Open Source est devenu planétaire et politique faisant intervenir de très nombreux acteurs. Nous sommes alors entrés dans une nouvelle ère, celle de la « guerre de l'information ».

Section 2) Des enquêtes citoyennes par le biais des réseaux sociaux

Certains citoyens, souhaitant protéger les enfants vulnérables sur les réseaux sociaux, ont créé des milices dans le but de lutter contre le phénomène de pédocriminalité (§1). Les communautés présentent sur les réseaux sociaux ont aussi donné naissance à des mouvements pour libérer la parole des femmes victimes de violences sexuelles (§2).

§1 La participation citoyenne dans la lutte contre la pédocriminalité

Bien que la transformation numérique ces dernières décennies a eu de nombreux effets bénéfiques sur notre vie courante, elle a aussi engendré de nombreux inconvénients. Parmi eux, la pédo-criminalité a trouvé un nouveau terrain d'exercice : Internet. Aujourd'hui, les pédophiles créent des faux comptes sur des réseaux sociaux tels que Facebook, Instagram ou Snapchat pour aborder les enfants par le biais de messageries instantanées et ensuite leur proposer notamment d'envoyer et de recevoir des photos ou vidéos de leurs parties intimes respectives et encore d'obtenir des faveurs sexuelles s'ils se rencontrent.

De cette façon, il est bien plus aisé pour ces criminels d'agir discrètement et leurs chances d'arriver à leurs fins ont été largement augmentées à l'ère du numérique. Auparavant, ils se rendaient à la sortie des écoles ou dans une aire de jeux par exemple où les parents et beaucoup de personnes étaient présents et pouvaient signaler les comportements suspects. Désormais, plus rien ne sépare le pédophile de l'enfant : en se faisant passer pour une fillette de 12 ans, la victime qui n'est pas mise en garde ne se méfie pas et cela la rend d'autant plus vulnérable. C'est pourquoi le législateur est intervenu dans l'objectif de réprimer cette délinquance moderne.

Ainsi, la pédopornographie telle qu'elle existe depuis toujours s'est vue transformée par l'arrivée des technologies numériques. Elle n'est pas définie par les textes de lois français mais la décision cadre de l'Union européenne du 22 décembre 2003 relative à la lutte contre l'exploitation sexuelle des enfants et la pédopornographie propose une définition commune.

D’après son premier article, la pédopornographie serait comprise comme « *tout matériel pornographique représentant de manière visuelle :- un enfant réel participant à un comportement sexuellement explicite ou s’y livrant, y compris l’exhibition lascive des parties génitales ou de la région pubienne d’un enfant, ou ; - une personne réelle qui paraît être un enfant participant ou se livrant au comportement visé au point i), ou ; - des images réalistes d’un enfant qui n’existe pas participant ou se livrant au comportement visé au point i).* »

Aujourd’hui, ce sont les articles 227-3, 227-22, 227-23 et 227-24 du Code Pénal qui sanctionnent ces comportements. Ainsi, pour exemple, l’article 227-22 du Code pénal dispose que « Le fait de favoriser ou de tenter de favoriser la corruption d'un mineur est puni de cinq ans d'emprisonnement et de 75 000 euros d'amende. Ces peines sont portées à sept ans d'emprisonnement et 100 000 euros d'amende lorsque le mineur a été mis en contact avec l'auteur des faits grâce à l'utilisation, pour la diffusion de messages à destination d'un public non déterminé, d'un réseau de communications électroniques ou que les faits sont commis dans les établissements d'enseignement ou d'éducation ou dans les locaux de l'administration, ainsi que, lors des entrées ou sorties des élèves ou du public ou dans un temps très voisin de celles-ci, aux abords de ces établissements ou locaux. »

De cette manière, non seulement le législateur réprime la corruption de mineur mais il aggrave sa répression lorsque l’auteur a utilisé un réseau de communication électronique.

Cependant, les moyens dont disposent les enquêteurs judiciaires pour lutter contre ces délinquants sont limités et ont dû être réadapté aux technologies numériques. Tout d’abord, les preuves de cette infraction sont difficiles à obtenir notamment concernant l’identité de l’auteur. En effet, contrairement aux infractions plus « classiques », les faits de pédopornographie commis par le biais d’Internet exigent des enquêteurs de trouver des preuves numériques. Ces dernières sont pourtant compliquées à recueillir en raison de leur caractère volatile, altérable et difficilement localisable.

De plus, les moyens d’enquête sont restreints dans un objectif de protection des libertés individuelles. En raison du caractère privé que revêtent les informations contenues dans les messages envoyés, il est nécessaire que la victime porte plainte pour que les services en soient informés. Cependant, les enfants, confrontés à ce type de corruption ne savent pas, pour la plupart, comment régir et sont très vulnérables. Ensuite, lorsque les services judiciaires sont informés de l’infraction, une seconde difficulté apparait. Pour obtenir l’identité de la personne à l’origine des messages il est primordial de parvenir à trouver son

adresse IP qui permet de remonter jusqu'à son auteur. Le problème réside dans le fait que les fournisseurs d'accès ne sont pas toujours coopératifs dans ces cas de figure.

Selon l'association Point de Contact, en 2019, la France était le troisième pays hébergeur de contenu à caractère pédopornographique mondial avec plus de 11 mille adresses de sites pédopornographiques. Selon les chiffres obtenus, 90% des victimes auraient entre 3 et 13 ans. En raison de la multiplication de ces comportements, des parents de victimes ainsi que d'anciennes victimes ont décidé de mener leurs propres enquêtes pour dénoncer ces pédo-criminels.

C'est de cette manière qu'ont commencé à se développer des milices numériques qui traquent les pédo-criminels en raison de la recrudescence de ces actes sur les réseaux sociaux. Appelés « chasseurs de pédophiles », ces citoyens agissent de façon bénévole et ont choisi de lutter à leur échelle pour protéger leurs enfants et ceux des autres.

Pour ce faire, et de la même façon que les enquêteurs judiciaires, ils enquêtent sous pseudonyme en créant des faux comptes d'enfants ou reprenant le compte d'une victime dans l'objectif de les appâter puis de les dénoncer aux services compétents.

C'est ainsi qu'en 2019, Steven Moore, un père de famille réunionnais, est devenu chasseur de pédophile en créant un faux profil de fillette prénommée Alicia. Puis, avec l'aide de deux personnes filmant la scène, il a confronté le premier pédophile présumé. Cette vidéo a permis aux services judiciaires d'arrêter le suspect et a été publiée sur les réseaux sociaux. C'est après cet épisode qu'il décide de créer la Team Moore dans le but de traquer les faux profils des pédo-criminels sur Facebook, monter un dossier sur eux avant de les remettre entre les mains de la Justice. Ces activistes sont désormais une cinquantaine et opèrent depuis la France, la Belgique et la Suisse.

Au commencement, Steven Moore s'est inspiré du phénomène existant dans les pays anglo-saxons. Au Royaume-Unis, les « chasseur de pédophile » collaborent activement avec la police qui tolèrent leur activité. C'est désormais la volonté de l'association : obtenir un cadre juridique légal pour exercer et ainsi être reconnu par l'Etat. Au Royaume-Uni, les militants travaillent d'ores et déjà en collaboration avec la police britannique, dans le but de compromettre numériquement des pédocriminels.

Leur objectif principal est de collaborer avec les services de police pour leur prêter main forte et non de se substituer à eux. Ils estiment que le système français est insuffisant pour lutter efficacement contre la recrudescence des pédophiles sur Internet.

C'est de cette manière qu'est née la Team Eunomie au sein de laquelle œuvrent désormais 37 internautes qui agissent à la fois en France et en Belgique. Ils constituent des dossiers au sein desquels ils classent les personnes en fonction de leur dangerosité à l'aide de 3 niveaux différents, le premier niveau correspondant aux plus dangereuses.

Bien que la plupart des délinquants pédophiles agissent seuls, la Team Eunomie a constaté que certains œuvrent par le biais de réseaux structurés. Ils ont ainsi découvert l'existence sur le Darknet d'un « *guide du pédophile* » qui donne aux internautes un mode d'emploi sur la manière de kidnapper une petite fille[116].

En juin 2021, Madame Maud Petit, députée à l'Assemblée nationale et soutenant l'association, a souhaité questionner le garde des sceaux, ministre de la Justice lors d'une question orale sans débat N°1522. La demande concernait l'instauration d'un cadre légal pour que la Team Moore et les citoyens concernés par la lutte contre les pédocriminels puissent travailler conjointement avec la police et la justice.

Pour appuyer sa demande, la députée précise que « Des profils factices de mineurs sont créés sur les réseaux, permettant de constater régulièrement des situations de pédocriminalité, en prenant soin de ne jamais provoquer au délit ». De cette manière, elle entend expliquer que les activistes respectent d'ores et déjà les règles de procédure pénale applicables aux enquêteurs judiciaires. Elle ajoute ensuite que « L'engagement citoyen sur le terrain n'est pas un phénomène nouveau : il existe en effet d'autres collectifs citoyens, tel que le dispositif « *voisins vigilants* », qui permet d'alerter les forces de l'ordre et d'accélérer l'intervention en cas de cambriolage ». En effet, les citoyens peuvent déjà apporter leur aide aux services de police pour améliorer le système judiciaire à leur échelle. En ce sens, la création d'un cadre légal permettant une collaboration entre les « chasseurs de pédophile » et les enquêteurs ne serait pas une première.

[116] Frédéric Durand, « En Normandie, les « chasseurs de pédophiles » enquêtent, les autorités se méfient », 2020, https://www.leparisien.fr/faits-divers/en-normandie-les-chasseurs-de-pedophiles-enquetent-les-autorites-se-mefient-23-09-2020-8389875.php

Cependant, même s'il reconnait que cette solution serait très efficace, la réponse de Monsieur Éric Dupond-Moretti fut négative. Il a ainsi considéré que « les risques de dérive sont très importants » en raison des garanties qu'il est nécessaire d'apporter au sein de la procédure pénale. C'est pourquoi, précise-t-il, « les policiers, les gendarmes et les magistrats qui s'occupent de cette question en ont appris la déontologie ; ils ont prêté serment et travaillent au service de la République ». Il ajoute que chacun doit rester à sa place et exercer son propre métier pour éviter les dérives dangereuses que représenterait l'intégration de citoyens dans le processus de procédure pénale.

Cet avis défavorable, bien que justifié par une volonté de protection de la procédure pénale, est fortement tranché. Le ministre de la Justice nous affirme vouloir prévenir des risques que ce cadre légal pourrait engendrer sans pour autant les définir. De plus, il précise que l'enquête sous pseudonyme prévue par le code de procédure pénale « se déroule sous contrôle du procureur de la République ou du juge d'instruction, ce qui offre de nombreuses garanties ». Pourtant, si ce contrôle permet d'offrir des garanties, pourquoi l'instauration d'un contrôle similaire ne pourrait-il pas en faire de même à l'égard des citoyens ?

La volonté des activistes est identique à celle des services judiciaires et ils œuvrent d'ores et déjà en aillant pour but de respecter la procédure pénale qui ne leur ait pourtant pas applicable. C'est pour cette raison qu'ils veillent à ne pas provoquer à l'infraction, action considérée comme déloyale et prohibée par la jurisprudence concernant une autorité publique. En effet, la Cour de cassation considère de manière constante que « le recours à la ruse ou à un stratagème, par un représentant de l'autorité publique, est déloyal s'il a pour objet ou effet de pousser à la commission de l'infraction qui, sans cela, n'aurait pas été commise »[117]. Cette décision des miliciens marque une réelle implication de la part de ces activistes dans leur collaboration ainsi que la conscience des responsabilités qui pèsent sur les enquêteurs.

En dehors de tout cadre légal, ces associations ne sont donc pas soumises au cadre légal prévu par le CPP. Se pose alors la question de la recevabilité de la preuve fournit lors des dénonciations par les chasseurs de pédophiles. Le code de procédure pénale pose le principe de liberté de la preuve dans son article 427 alinéa premier qui dispose que « hors les cas où la loi en dispose autrement, les infractions peuvent être établies par tout mode de preuve et le juge décide d'après son intime conviction ». Cependant, ce principe n'est pas absolu et

[117] Arrêt n° 650 du 9 déc. 2019, 18-86.767

s'applique différemment en fonction de l'auteur de la preuve. Plus précisément, une autorité judiciaire aura pour obligation de respecter un principe de loyauté dans l'administration de la preuve tandis que la preuve obtenue par une personne privée de façon déloyale ou illicite ne pourra être écartée pour ce seul motif.

Sur ce point, comme l'a relevé Simon Takoudju dans son article intitulé « *Les règles de droit face à la pédopornographie 2.0.* », la jurisprudence est constante. En effet, dans un arrêt du 30 mars 1999 (n°97-83.464) la Cour de cassation affirmait que « *la circonstance que des documents ou des enregistrements remis par une partie ou un témoin aient été obtenus par des procédés déloyaux ne permet pas au juge d'instruction de refuser de les joindre à la procédure, dès lors qu'ils ne constituent que des moyens de preuve qui peuvent être discutés contradictoirement* ».

De plus, dans un arrêt du 27 janvier 2010 (n°09-83.395) elle complétait son raisonnement en précisant « *qu'aucune disposition légale ne permet aux juges répressifs d'écarter des moyens de preuve remis par un particulier aux services d'enquête, au seul motif qu'ils auraient été obtenus de façon illicite ou déloyale et qu'il leur appartient seulement, en application de l'article 427 du code de procédure pénale, d'en apprécier la valeur probante, après les avoir soumis a la discussion contradictoire* ».

De cette façon, une personne privée ne sera pas soumise au principe de loyauté auquel doit répondre une autorité judiciaire. C'est le principe de liberté de la preuve qui prévaut et qui leur sera appliqué selon la chambre criminelle.

En définitive, les milices privées possèdent plus de moyens que les services judiciaires dans la recherche et l'obtention de preuves en vue d'établir la vérité. Les règles de procédures ne sont pas aussi strictes notamment parce qu'une autorité judiciaire doit respecter une certaine déontologie en tant que représentant de l'Etat. Ces milices privées possèdent donc un avantage de taille, elles peuvent se procurer des preuves par des moyens auxquels n'ont pas accès les forces de l'ordre.

Difficultés. Si les enquêteurs privés parviennent à découvrir l'identité de nombreux délinquant pédophiles, la Gendarmerie Nationale averti sur les difficultés concernant les suites judiciaires. En effet, le Centre de Lutte contre les Criminalités Numériques C3N a rappelé « *que la cyberinfiltration est née en 2007. Le législateur a permis aux enquêteurs de bénéficier de techniques spéciales pour confondre des pédocriminels avant qu'ils ne passent à l'acte et donc de protéger des enfants. En termes de droit français, cela s'appuie sur la recevabilité de la preuve qui doit être recueillie de façon légale. Pour cela, il y a trois choses à faire en cyberinfiltration : être formé, être habilité, être dans un service spécialisé par un arrêté* ».[118]

L'un des problèmes majeurs réside dans le fait qu'il n'est pas possible de se reposer sur les dossiers qu'ils montent puisque le juge doit s'appuyer sur un dossier solide pour prononcer une sanction. Ainsi, le militaire qualifie leurs enquêtes de « contre-productive dans l'exercice de la police judiciaire » et rappelle que la poursuite d'une enquête requiert du temps mais aussi plusieurs étapes primordiales. C'est pourquoi l'identification correspond seulement à la première phase de l'enquête lors de laquelle il faudra « ajouter la réalisation d'un environnement complet sur la cible ». Enfin, il affirme que si le début des investigations est bancal ou déloyal, la procédure pourra être cassée ou bien utilisée par les avocats de la Défense.

[118] Pôle Judicaire de la Gendarmerie Nationale, Les cyber-enquêteurs alertent sur les difficultés levées par les «chasseurs de pédophiles», https://www.gendarmerie.interieur.gouv.fr/pjgn/actualite/vu-dans-les-medias/les-cyber-enqueteurs-alertent-sur-les-difficultes-levees-par-les-chasseurs-de-pedophiles

§2 Les outils numériques au service des victimes de violences sexuelles

Un second type de délinquance s'est retrouvé au cœur d'un phénomène de grande ampleur sur Internet : le harcèlement sexuel. De nombreux mouvements de mobilisation sur les réseaux sociaux tels que « MeToo » et « Balancetonporc » se sont développés dans l'objectif de lutter contre les délinquants sexuels.

C'est l'article 222-33 du Code pénal qui définit le harcèlement sexuel comme « *le fait d'imposer à une personne, de façon répétée, des propos ou comportements à connotation sexuelle ou sexiste, qui soit porte atteinte à sa dignité en raison de leur caractère dégradant ou humiliant, soit créent à son encontre une situation intimidante, hostile ou offensante* ».

Les articles 222-22 et suivants du code pénal réprime les infractions sexuelles telles que les agressions sexuelles, viols et atteintes sexuelles. Cependant, la dénonciation de ces actes ainsi que le processus judiciaire que les victimes doivent affronter posent plusieurs problématiques.

En effet, les agressions sexistes et sexuelles font l'objet de passages sous silences, de non-dit essentiellement parce que les femmes qui en sont victimes sont psychologiquement fragilisées. C'est pourquoi il arrive souvent que la honte, la peur du rejet de la société et de leurs proches ou de leur non-croyance sont des obstacles considérés par elles comme infranchissables. Ces infractions sont donc peu dénoncées aux services judiciaires, la narration de leur agression étant trop difficile devant des figures d'autorité, les victimes ne relatant souvent même pas les faits à leurs proches.

De plus, le processus judiciaire est long et oblige les victimes à se retrouver en confrontation avec leur agresseur. La production de preuves est souvent pauvre soit parce que les faits se sont déroulés des années auparavant, soit par absence de témoin ou de séquelles physiques pouvant être constatées par un expert. Cette délinquance se déroule souvent à huit clos, la femme ne disposant que d'une seule arme au procès : sa parole. C'est pour cette raison qu'il arrive qu'elle ne soit pas crue et même accusée de diffamation. Il est difficile d'établir de façon certaine la question de savoir : qui dit la vérité ?

En France, la présomption d'innocence est un principe de valeur constitutionnelle[119], prévu par l'article préliminaire du code de procédure pénale qui dispose que "*La*

[119] Cons. const. 8 juill. 1989, n° 89-258 DC et Cons. const. 2 mars 2018, n° 2017-693 QPC

présomption d'innocence est le principe selon lequel toute personne, qui se voit reprocher une infraction, est réputée innocente tant que sa culpabilité n'a pas été légalement démontrée."

De cette manière, la présomption d'innocence interdit de présenter une personne comme coupable avant qu'elle ait été jugée comme tel par une juridiction. Dans le prolongement de cette idée, le juge doit s'abstenir de condamner une personne lorsqu'il n'a pas suffisamment de preuves de sa culpabilité. Autrement dit, lorsque le juge a un doute quant à la culpabilité d'une personne, il ne pourra pas la condamner. C'est dans ce contexte qu'on utilise l'expression « le doute profite à l'accusé ».

Les victimes de cette délinquance, qui ne possèdent pas assez de preuves pour s'assurer de la condamnation de leur agresseur, sont alors souvent découragées et préfèrent baisser les bras avant de s'engager dans un processus qui prendra probablement des années et qui les obligera à relater les faits devant de nombreuses personnes ainsi que de se faire malmener lors des confrontations avec l'avocat de la défense.

Il arrive aussi que certaines femmes ne franchissent pas l'étape suivant le dépôt de plainte. Rattrapée par la peur, la honte, découragée par ses proches ou même son agresseur, la victime peut retirer sa plainte. Ce sont autant d'éléments représentant un obstacle à l'endossement de la responsabilité de l'auteur que la Justice permettrait.

C'est pourquoi, certaines victimes ont décidé de prendre le pas sur cette omerta et de mobiliser les réseaux sociaux et leurs communautés pour changer les choses. Le 5 octobre 2017, le New York Times publie des témoignages de plusieurs actrices révélant avoir été harcelées par le producteur Américain Harvey Weinstein. Suite à ces révélations, le 8 octobre, il est licencié par le conseil d'administration de son entreprise. Quelques jours après, le New Yorker publie une enquête de fond sur ces accusations. Cependant, les témoignages de harcèlement sexuel, d'agressions et de viols s'accumulent contre le producteur révélant une affaire de grande ampleur.

Alyssa Milano, actrice Américaine et victime du producteur, relance alors le mouvement dénommé MeToo créé dix ans auparavant par Tarana Burke, une militante féministe américaine. Son objectif est d'encourager les victimes de violences sexuelles à écrire leurs témoignages suivis de l'hashtag MeToo pour leur permettre de libérer leurs paroles. Son message est alors partagé des dizaines de millions de fois en quelques jours et il prend une dimension virale sur les réseaux sociaux.

Par la suite les agresseurs sont dénoncés massivement, mais les victimes ne sont pas que des femmes. C'est le cas de Kevin Spacey, accusé le 29 octobre 2017[120] par l'acteur Anthony Rapp de lui avoir fait des avances sexuelles en 1986 alors qu'il était âgé de 14 ans. En réponse, il publie une lettre dans laquelle il reconnait les faits, présente ses excuses mais tente de se justifier dans le même temps.

A la suite de ces révélation, l'acteur Kevin Spacey est retiré de la série « House of Cards » dans laquelle il joue le rôle principal ainsi que du film « Tout l'argent du monde » dans lequel ses scènes ont été effacées. D'autres faits similaires sont dénoncés au Royaume Unis et aux Etats-Unis.

Partagé à l'échelle planétaire, et encouragé par les confessions d'actrices mondialement connues, des millions de femmes ont alors avoué avoir été victimes de ces mêmes abus et ont raconté leur histoire. En France, le mouvement, lancé par Sandra Muller, se nomme #balancetonporc et enjoint les femmes à briser l'omerta sur les agressions sexuelles mais aussi le sexisme quotidien. La journaliste enjoint les victimes à dénoncer publiquement, sur les réseaux sociaux, leurs agresseurs en donnant leurs noms. L'hashtag aussi été repris en espagnol (#Yo Tambien) et connais des dérivations #WhatWhereYouWearing ou par exemple #TimesUp.

La multitude de témoignages de femmes rassemblées sous cet hashtag a engendré une prise de conscience à l'échelle internationale du phénomène de harcèlement sexuel. Mais l'impact de ces révélations ne s'est pas arrêté là puisque, deux ans après le lancement du mouvement, ce sont sur, de façon plus générale, toutes les formes de violence envers les femmes qui ont été dénoncées.

Ces multiples mouvements n'enjoignent pas seulement la parole des victimes puisqu'un autre hashtag est ensuite apparu : #HowIWillChange créé par l'écrivain Benjamin Law également en 2017. Celui-ci a souhaité que les hommes endossent leurs responsabilités et assument leurs actes en reconnaissant publiquement leurs agissements.

[120] Dans un article du site BuzzFeed

En 2020, Harvey Weinstein a été reconnu coupable d'agressions sexuelles ainsi que de viols par un tribunal de New York puis condamné à 23 ans de prison. Cette décision démontre que ce mouvement social n'a pas seulement permis de briser l'omerta et de libérer la parole des femmes mais qu'il a permis au producteur de rendre compte de ses agissements devant la Justice et d'être condamné en conséquent.

Le mouvement MeToo ne s'est pourtant pas arrêté là : en 2018, l'initiative Time'Up portée par des 300 femmes du milieu du divertissement est annoncée. Son objectif est de créer un fond légal de défense dans le but de soutenir financièrement les victimes d'agression sexuelle et de harcèlement tout au long du processus judiciaire[121]. Elle soutient les femmes ayant trop peu de moyens financiers pour se défendre. Plus généralement, l'organisation milite pour obtenir plus de parité notamment dans le milieu du travail, appelant les entreprises à modifier leurs règlementations sur le harcèlement.

[121] Christine Vainqueur, « Le mouvement #MeToo », https://www.marieclaire.fr/le-mouvement-me-too,1361950.asp

Chap 2 Les défis engendrés par le développement d'une justice citoyenne

Les enquêtes modernes effectuées par les citoyens par le biais de l'Open source Intelligence et des réseaux sociaux a engendré de nombreux défis notamment le risque grandissant d'un passage de l'Etat de droit vers un Etat régit par une justice privée (section 1). C'est pourquoi, il est aujourd'hui primordial de définir un encadrement juridique relatif à cette justice moderne émergente (section 2).

Section 1 Les risques d'une évolution vers un état de droit régit par une justice privée

L'apparition d'une justice citoyenne rénovant les techniques d'enquêtes remet d'ores et déjà en question les procédures judiciaires classiques (§1) et finit par engendrer l'apparitions de nouvelles règles juridiques procédurales démontrant une influence indéniable sur le droit positif (§2).

§1 Une remise en question des procédures judiciaires contemporaines

La preuve. L'apparition et le développement massif des investigations journalistiques à partir de l'Open Source ainsi que des enquêtes citoyennes dans un but de répression des auteurs d'infractions ont désormais pris tellement d'importance qu'ils remettent en question des procédures judiciaires actuelles. C'est aussi le cas concernant les techniques d'enquêtes des services judiciaires.

L'un des exemples les plus parlant dans ce processus concerne l'étape de la recherche des preuves. Il existe ainsi une différence importante de régime entre personne privée et autorité privée s'agissant du devoir de loyauté dans la recherche des preuves. La loyauté est un principe essentiel dans la poursuite de la vérité en matière de procédure pénale. Pourtant, ce principe ne s'applique pas à tous les acteurs du procès. C'est notamment le cas de la personne

poursuivie qui bénéficie du droit au silence ainsi que de la possibilité de mentir[122]. Mais ce principe ne s'applique pas non plus aux personnes privées recherchant des preuves par leurs propres moyens.

Tout d'abord, l'autorité publique est soumise au principe de loyauté dans la recherche des preuves. En principe, les officiers de police judiciaire ne peuvent jamais, tant en enquête de flagrance ou préliminaire, procéder à des écoutes téléphoniques, même avec l'accord d'un des correspondants sur la ligne duquel est installé le système d'écoute[123]. Seul le juge peut prendre la décision de placer sur écoute téléphonique un individu.

Ce principe ne s'applique cependant pas dans le cas où les policiers n'ont pas provoqué à l'infraction. En effet, dès lors qu'ils ont une attitude passive et que seules les parties privées procèdent à un enregistrement « clandestin », cela ne constitue pas une violation du principe de loyauté. La Cour de cassation reconnait que « *le concept de "participation", même indirecte, suppose l'accomplissement, par les enquêteurs d'un acte positif, si modeste soit-il* » et que « *le seul reproche d'un "laisser faire" des policiers, dont le rôle n'a été que passif, ne peut suffire à caractériser un acte constitutif d'une véritable implication* » [124]. De cette façon il faut distinguer selon que la participation de l'autorité publique ait été directe ou indirecte lors de l'enregistrement.

La jurisprudence reconnait cependant que l'autorité publique puisse fournir en justice des enregistrements clandestins, faits à l'insu de la personne poursuivit, uniquement si elle est soumise à la libre discussion des parties et qu'elle ne constitut qu'un élément probatoire laissé à l'appréciation des juges[125].

Une personne privée, quant à elle, n'est pas soumise au principe de loyauté dans la recherche des preuves depuis une série d'arrêts intervenus après les années 1990. Pour ces dernières, c'est le principe de liberté qui prévaut. A la différence d'une autorité publique, une personne privée peut donc rapporter une preuve obtenue de façon déloyale c'est à dire à l'insu de la personne poursuivie ou bien en provoquant la personne à l'infraction.

---

[122] Reconnu depuis l'arrêt Funke c/France 25 février 1993 rendu par la Cour européenne des droits de l'homme sur le fondement de l'article 6 de la Convention européenne des droits de l'homme.
[123] V. Paris, 8 févr. 1995, aff. Schuller/Maréchal, D. 1995. 221, note Pradel. – Puis arrêt de rejet : Crim. 27 févr. 1996, no 95-81.366, D. 1996. 346, note Guéry ; JCP 1996. II. 22629, note Rassat
[124] Cass., ass. plén., 10 nov. 2017, no 17-82.028 , JCP 2017. 1376, obs. C. Ribeyre ; JCP déc. 2017, no 52, p. 1366, obs. A. Gallois ; Procédures janv. 2018, no 1, comm. 23, obs. Chavent-Leclère ; D. 2018. 103, note Décima ; AJ pénal 2018. 100, obs. Kurek
[125] Crim. 13 oct. 2004, no 00-86.726 , Bull. crim. no 243

Ainsi, alors que des garanties entourent le recours au recueil des aveux par les autorités policières ou judiciaires, ce n'est pas le cas de l'aveu obtenu par une personne privée. De cette manière, en plus de disposer de technologies numériques plus étendues que les services d'enquête de police, les citoyens disposent d'un champ d'intervention plus important que les autorités publiques de la recherche des preuves. Plus simplement, ces derniers possèdent beaucoup plus de moyens à la fois pour enquêter sur des infractions mais aussi pour en rapporter la preuve aux autorités judiciaires. Cela représente un paradoxe assez étonnant.

Alors même que les citoyens ne sont pas habilités par la loi à mener des investigations sur des infractions, l'absence de cadre législatif strict peut conduire les citoyens à devenir les nouveaux enquêteurs de demain.

Collaboration entre secteur privé et secteur public. Cette situation peut aussi aboutir, dans un objectif de perfectionnement des techniques d'enquêtes, au développement d'une coopération entre le secteur privé et le secteur public. Une telle association permettrait d'apporter une plus-value non négligeable aux moyens de lutte contre la délinquance. Dans cet ordre d'idée, les sociétés privées pourraient apporter au secteur public leur expertise dans un domaine auquel les enquêteurs n'ont pas accès.

C'est d'ores et déjà le cas du groupe Deveryware, société privée créé en 2003, qui est un expert en technologies d'investigation et des services pour la sécurité globale. Il s'est engagé à servir la sécurité des Etats, des entreprises et des populations par des technologies numériques innovantes et des solutions adaptées.

Il se considère aujourd'hui comme un « *accélérateur d'enquêtes qui accompagne les forces de l'ordre dans la détection et la prévention des menaces. Deveryware met à disposition des solutions numériques répondant à leurs besoins d'accélérer les investigations, d'analyser les preuves* »[126]. De cette manière, il permet d'apporter, à l'aide de technologies modernes d'investigation numérique et de services pour la sécurité globale, un soutien aux enquêtes policières. Pour cela, il dispose de témoignages ainsi que de l'analyse de nombreux experts dans le domaine de la sécurité.

Le 14 octobre 2020, la société publie son livre blanc intitulé « *Le Data au cœur de l'enquête* » dans le but d'apporter des réponses aux questions d'actualité qui entourent le

[126] « Le groupe Deveryware », 2020, https://www.tracip.fr/le-groupe-deveryware/

traitement des données par les enquêteurs. Ce livre se propose d'apporter plusieurs constats effectués par divers spécialistes.

Les auteurs estiment qu'un renforcement de la coopération entre acteurs étatiques et industriels, européens et internationaux est souhaitable. Selon le groupe Deveryware « *Ils doivent pouvoir évoluer dans des cadres techniques, réglementaires, éthiques et financiers transparents et cohérents. La France est confrontée à un enjeu de souveraineté technologique. Encourager une coopération public-privé et s'appuyer sur une vision stratégique commune constituent des solutions pour répondre à cet enjeu* »[127].

Aujourd'hui, les enquêtes effectuées par les journalistes par le biais de l'Open Source nous ont permis de constater que les investigations policières classiques (écoutes téléphoniques, géolocalisation d'un téléphone…) pouvaient être regardées sous un nouveau jour. L'analyse que les journaux tels que Le Monde ou encore la BBC nous offrent lorsqu'ils démontrent les étapes successives qui leur ont permis d'identifier les éléments essentiels d'une infraction, seulement à partir de simples photographies et vidéos postées sur les réseaux sociaux, apporte une vision modernisée de la conduite des enquêtes judiciaires.

Autrement dit, les techniques dites d'Open Source Intelligence représentent une source non négligeable des outils disponibles et librement accessibles au sein des procédures judiciaires.

§2 L'influence des réseaux sociaux sur le droit

Les technologies numériques n'ont pas seulement bouleversé notre quotidien, elles ont aussi pris une part de plus importante au sein de notre droit. Comme vu précédemment, de nombreux citoyens et sociétés privées œuvrent dorénavant pour lutter contre des phénomènes de criminalité qui touchent particulièrement notre société (harcèlement sexuel, pédopornographie…). Chaque mouvement citoyen créé à partir d'un réseau social tente, avec les moyens dont il dispose, de participer à rendre une Justice plus efficace.

[127] Le groupe Deveryware, « Le Groupe Deveryware publie son livre blanc « La Data au cœur de l'enquête », 2020, https://deveryware.com/wp-content/uploads/2020/10/CP-DEVERYWARE-Livre-Blanc-la-data-au-coeur-de-lenquete.pdf

Cependant, en tant que nouveauté, le droit n'était pas adapté à tout ce que ces mouvements sociaux et enquêtes privées ont engendré. En tant que matière vivante, elle est sans cesse en train d'évoluer et de s'adapter aux mœurs de la société.

Se pose aujourd'hui une nouvelle question, l'opinion public est-il devenu un juge dont les réseaux sociaux serait le tribunal ? Il est de plus en plus récurant que l'opinion public, manifesté par le biais des réseaux sociaux, vienne perturber le déroulement d'un procès ou d'une enquête judiciaire.

L'exemple le plus marquant en France fut le procès de Jacqueline Sauvage. Elle a été reconnue coupable du meurtre de son mari violent et condamnée à 10 ans de réclusion criminelle par la cour d'assise du Loiret, confirmée en appel. Pendant quarante-sept ans, elle avait subi les violences psychologiques, physiques et sexuelles de son mari qui avait abusé d'elle et de leurs trois filles. Jacqueline Sauvage est alors devenue un emblème des victimes de violences conjugales.

Une mobilisation populaire se met alors en place et les réactions sur les réseaux sociaux sont de grande ampleur sous le #LibérerJacquelineSauvage. Elle est considérée par l'opinion public en tant que victime et non comme coupable. Un comité de soutien est aussi créé, dont faisaient partis des figures politiques (Anne Hidalgo, Daniel-Bendit et Jean Luc Mélanchon), pour obtenir sa libération. Des artistes se mobilisent aussi aux côtés de très nombreux citoyens qui partagent leurs avis sur les réseaux sociaux ainsi que dans les médias.

Face à ce mouvement populaire de grande ampleur, le président de la République[128] décide alors de lui accorder une grâce partielle pour lui permettre de faire une demande de libération conditionnelle. Refusée par le tribunal d'application des peines, la mobilisation nationale amène François Hollande à lui accorder une grâce totale le 28 décembre 2016.

Ce choix a été très critiqué par les juristes, notamment parce que le président de la République a choisi de soutenir l'opinion publique plutôt qu'une décision rendue par une juridiction judiciaire. Les réseaux sociaux marquent ici un tournant important pour la Justice. Leur influence lors de ce procès s'est concrétisée par un impact réel dans la Justice. C'est une preuve du poids incontestable que peut représenter l'opinion public auprès des politiciens à l'ère des réseaux sociaux.

[128] François Hollande à l'époque

La présomption d'innocence. L'influence des réseaux sociaux peut aussi avoir un impact important vis-à-vis de la présomption d'innocence. En effet, le phénomène viral n'a pas eu seulement des effets positifs comme la libération de la parole des femmes mais aussi des effets négatifs. Prenons pour exemple un procès très médiatisé impliquant l'acteur Johnny Depp.

Un second impact s'est retrouvé, lors du procès opposant Johnnyp Depp à son ex-femme Amber Heard. Si les violences faites aux femmes sont aujourd'hui reconnues et de plus en plus dévoilées, cela engendré un phénomène inverse inquiétant. En effet, lorsqu'Amber Heard avait accusé Johnny Depp d'être l'auteur de violences conjugales, avant même qu'un jugement l'ait reconnu coupable, les studios Disney ont décidé d'arrêter toute collaboration avec l'acteur. Au moment même où le mouvement MeToo était en plein essors, les studios ont préféré se protéger de l'opinion public. Cependant, lorsque Johnny Depp a démenti ses propos et l'a accusée de diffamation et de violence physiques et psychologiques, les tribunaux judiciaires ont dû répondre à la question de savoir : qui est responsable de quelles violences à l'encontre de son ex-époux ? Et, dans quelle mesure ?

En parallèle du procès judiciaire des ex-époux, se déroule alors le procès de l'opinion. Les audiences étant transmises en direct, des millions d'internautes ont publié leur avis sur la question et ont déterminé qui était le coupable et la victime. Une pétition mise en ligne pour qu'Amber Heard soit exclue du prochain film « Aquaman » a atteint 4 millions de signatures. Par le biais de cette dernière, les internautes ont tenté d'obtenir justice en condamnant l'actrice par leurs propres moyens. Pour l'opinion public, le procès était déjà terminé et le jugement rendu avant même que la juridiction se soit prononcée : c'est Amber Heard mentait en accusant son ex-époux de violences physiques et psychologiques. Ainsi, peu importe ce que le tribunal judiciaire a décidé, le tribunal de l'opinion avait déjà tranché.

Ne serait-ce pas là l'illustration de l'influence de l'opinion publique sur le droit ? Le mouvement social MeToo qui a pour but de libérer la parole des femmes victimes de violences sexuelles n'aurait-il pas eu pour impact de juger trop rapidement Johnny Depp ? On assiste alors, pour la première fois depuis l'apparition du mouvement à un nouveau phénomène : la prise de conscience générale des cas de diffamation. Cependant, il est primordial que le tribunal médiatique ne se substitue pas au tribunal judiciaire.

Les dérives des mouvements des réseaux sociaux. Un article intitulé « *Derrière le respect de la dignité de la personne humaine, le retour du gouvernement des juges* ? » écrit par Pierre Esplugas-Labatut, Professeur à l'université Toulouse-I-Capitole, vient mettre l'accent sur l'une des dérives dangereuses de ces mouvements de mobilisation. L'exemple sur lequel se base son argumentation est celui de trois ordonnances de référé rendues le 7 décembre 2021 par le tribunal administratif de Toulouse.

En l'espèce, deux tableaux avaient été exposés au centre hospitalier universitaire de Toulouse-Purpan. Ils mettaient en scène des membres du centre dans des positions sexuelles telles qu'un homme tenu en laisse par une femme avec un fouet à la main. Deux associations féministes et un syndicat avaient saisi le tribunal au motif que ces tableaux heurtaient le principe de dignité de la personne humaine en raison de leur caractère pornographique.

Le professeur fait grief au juge d'avoir reconnu l'atteinte à la dignité alors que selon lui « *nous assistons à un glissement car c'est le juge et non l'autorité politique qui apprécie le caractère pornographique ou non de la fresque* ». S'il reconnait le caractère de service public de l'établissement, induisant selon lui une forme de neutralité justifiant sa décision, il lui reproche de « *concevoir la neutralité comme une abstention dans la monstration de scènes sexuelles* ». Il rapproche même cette décision de censure d'œuvre d'art à l'absence de liberté des régimes autoritaires.

Concluant que ce jugement fait probablement écho aux mouvements de défense des valeurs féministes telles que #MeToo, il craint cependant « *un inquiétant retour, sous couvert de féminisme, (…) d'un gouvernement des juges* »[129].

Le mouvement social #Metoo prône des valeurs louables que représentent la défense des femmes et leur prise de parole. Pourtant, au vu de l'ampleur prise par ce mouvement, des dérives peuvent rapidement en découler et assombrir le décor. C'est exactement ce que le professeur tente de mettre à jour et de prévenir. La prise de position du juge administratif dans cet arrêt est un exemple des risques que peuvent engendrer les mouvements sociaux numériques. Le juge prend un rôle discutable, lui appartient-il de déterminer le caractère

[129] Pierre Esplugas-Labatut, « Derrière le respect de la dignité de la personne humaine, le retour du gouvernement des juges ? », *AJDA*, https://www-dalloz-fr.lama.univ-amu.fr/documentation/Document?ed=etudiants&ctxt=0_YSR0MD1tZXRvb8KneCRzZj1zaW1wbGUtc2VhcmNo&ctxtl=0_cyRwYWdlTnVtPTHCp3MkdHJpZGF0ZT1GYWxzZcKncyRzb3J0PSNkZWZhdWx0X0Rlc2PCp3Mkc2xOYlBhZz0yMMKncyRpc2Fibz1UcnVlwqdzJHBhZ2luZz1UcnVlwqdzJG9uZ2xldD3Cp3MkZnJlZXNjb3BlPUZhbHNlwqdzJHdvSVM9RmFsc2XCp3Mkd29TUENIPUZhbHNlwqdzJGZsb3dNb2RlPUZhbHNlwqdzJGJxPcKncyRzZWFyY2hMYWJlbD3Cp3Mkc2VhcmNoQ2xhc3M9wqdzJHRhYlJmdD03M0Q1QTkzQg%3D%3D&id=AJDA%2FCHRON%2F2022%2F0355

immoral ou non d'une œuvre alors qu'il est autorité judiciaire et non politique ? La réponse est bien sûr négative.

Une influence sur le droit constitutionnel. Les nouveaux Cahiers du Conseil constitutionnel n° 57 intitulés « *Le numérique : un défi pour le droit constitutionnel* »[130] envisagent, au regard de l'impact des réseaux sociaux dans le monde, un nouveau processus d'expression de la souveraineté et de construction du débat démocratique. Les auteurs affirment en effet que la démocratie connectée aussi appelée « e-*democracy* » permet de nouvelles perspectives concernant l'exercice des droits civils et politiques. Ils s'appuient sur l'apparition de votes électroniques, de droits de pétition, d'appels à contribution ou encore de consultations publiques se développant massivement sur les réseaux.

Le « *crowdsourcing* » est une méthode de production participative issue du marketing qui permet de « *valoriser les idées et expériences du plus grand nombre dans les processus décisionnels et réanime l'idéal de la démocratie directe* »[131]. Il a été rendu matériellement possible notamment grâce aux réseaux sociaux. Chaque citoyen peut être informé, consulté et associé au processus en fonction des cas. Les autorité politiques peuvent les appeler à proposer une loi ou, dans d'autres cas à l'enrichir, l'évaluer ou la valider.

Les auteurs pensent que cette méthode peut « *aider à reconnecter les élus aux citoyens, à mieux légitimer les processus décisionnels en faisant appel à l'expérience du terrain, à l'expertise des praticiens et des usagers, à la diversité des points de vue* »[132]. L'outil numériques a ainsi permis de faire évoluer la vie politique à l'égard des citoyens mais aussi des politiciens qui ont changé leur manière de « faire » de la politique.

Cet outil peut être considéré, à de multiples égards, comme un atout pour nos démocraties, un outil permettant de la revivifier.

[130] Julien BONNET, Pauline TÜRK, « Nouveaux Cahiers du Conseil constitutionnel n° 57 (dossier : droit constitutionnel à l'épreuve du numérique) », 2017, https://www.conseil-constitutionnel.fr/nouveaux-cahiers-du-conseil-constitutionnel/le-numerique-un-defi-pour-le-droit-constitutionnel

[131] Julien Bonnet et Pauline Türk, « Le numérique : un défi pour le droit constitutionnel », 2017, https://www.conseil-constitutionnel.fr/nouveaux-cahiers-du-conseil-constitutionnel/le-numerique-un-defi-pour-le-droit-constitutionnel

[132] 119 bis

De cette manière, les réseaux sociaux font désormais partie intégrante de notre quotidien, et sont un atout pour la démocratie, ils sont devenus un outil permettant de renouveler cette dernière.

Section 2) La nécessité d'un encadrement juridique pour prévenir ces risques

§1 Une limitation des droits des enquêteurs citoyens prévue par le RGPD

Au sein de l'Union européenne, le traitement des données personnelles est soumis à un règlement[133] qui encadre les droits des personnes concernées autant que la responsabilité de ceux qui récoltent les données.

Dans ce contexte, la notion de donnée personnelle doit être entendue au sens large. Elle correspond à « *toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée « personne concernée ») ; est réputée être une «personne physique identifiable» une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale* »[134]. Comme nous avons pu le voir, la numérisation ainsi que l'usage quotidien des technologies modernes a augmenté de façon exponentielle le recueil et le traitement de ces données personnelles.

Le terme de traitement signifie quant à lui « *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*

[133] Règl. (UE) n° 2016/679 du 27 avr. 2016
[134] CNIL, « Chapitre I - Dispositions générales », https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre1#Article1

toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction »[135].

En octobre 2008, lors de la 30ème conférence mondiale des commissaires à la protection des données et de la vie privée, il a été constaté que les utilisateurs de réseaux sociaux « ignorent le plus souvent les conséquences d'une large diffusion d'informations très personnelles »[136]. De plus, il a été remarqué qu'il n'existe, à ce jour, que « très peu de protection contre la copie de toute sorte de données personnelles des profils d'utilisateurs ». Par ailleurs, il peut s'avérer très difficile de retirer certaines informations du web une fois qu'elles ont été publiées et, la plupart du temps, ces mêmes données sont tout de mêmes accessibles par le biais d'un moteur de recherche.

La mise en place du droit au sein de cet espace dématérialisé est donc récente et le législateur a souvent été en retard sur l'évolution sociétale laissant ainsi des vides juridiques dont les sociétés ont pu tirer profit. Le règlement général sur la protection des données (RGPD) a apporté une réponse européenne concernant l'encadrement du traitement des données personnelles, précisant le cadre de ces nouveaux usages. Ainsi, le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données est entré en vigueur, a abrogé la directive de 1995 relatif au règlement général sur la protection des données.

Pour son élaboration, le législateur s'est appuyé sur l'article 8 de la charte des droits fondamentaux de l'Union européenne qui dispose que « *Toute personne a droit à la protection des données à caractère personnel la concernant. Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification. Le respect de ces règles est soumis au contrôle d'une autorité indépendante.* »

Le RGPD est ainsi applicable à tout « *traitement de données à caractère personnel, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier* »[137]. Autrement dit, les

[135] Idem 122
[136] G29, avis 5/2009, 12 juin 2009
[137] Article 4.2 du RGPD

données à caractère personnel sont couvertes par la protection du règlement dès lors qu'elles font l'objet d'un traitement automatisé. Ce sont plus précisément les technologies de l'information comme les réseaux de télécommunication, l'informatique, la géolocalisation par exemple.

Le RGPD est articulé autour de plusieurs axes que sont « le principe de transparence : l'information sur l'usage qui sera fait des données doit être complète, les données doivent être aisément accessibles pour être consultées, modifiées ou supprimées (droit à l'oubli) ; la minimisation des données : ne doivent être récoltées que les données utiles pour l'utilisation consentie par l'usager ; la limitation de la conservation des données : les données ne peuvent pas être conservées plus longtemps que la période nécessaire aux utilisations consenties par l'usager ; la sécurité et la confidentialité des données : les données doivent être stockées dans des emplacements sécurisés qui garantissent leur confidentialité »[138].

La CNIL a pour mission de contrôler la conformité des lois françaises au RGPD. Selon elle, le RGPD possède trois objectifs distincts : « la protection des personnes physiques à l'égard du traitement des données à caractère personnel et des règles relatives à la libre circulation de ces données ».

Mais aussi la protection des « libertés et droits fondamentaux des personnes physiques, et en particulier leur droit à la protection des données à caractère personnel. »

Et enfin, « La libre circulation des données à caractère personnel au sein de l'Union n'est ni limitée ni interdite pour des motifs liés à la protection des personnes physiques à l'égard du traitement des données à caractère personnel. »

C'est pourquoi désormais, l'utilisation des données à caractère personnel doit être explicitement consentie. Un exemple que l'on rencontre depuis la mise en place du RGPD est la présence de bandeaux requérant l'acceptation des cookies préalablement à la consultation d'un site web.

L'affaire Cambridge Analytica c/Facebook concernait la société Cambridge Analytica qui était accusée d'avoir recueillis et utilisé les données de dizaines de millions d'utilisateurs de Facebook obtenues sans leur consentement dans le cadre de la campagne électorale de Donald Trump. Pour ce faire, l'entreprise est passée par un quiz qui non seulement récoltait

[138] Idem 134

les données des participants mais aussi de leurs amis Facebook. Par la suite le G29 a créé un groupe dédié à la surveillance des diverses pratiques des réseaux sociaux.

L'article 5 du RGPD « Principes relatifs au traitement des données à caractère personnel » prévoit que « *les données à caractère personnel doivent être :*

a) traitées de manière licite, loyale et transparente au regard de la personne concernée

b) collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités ;

c) adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées ;

d) exactes et, si nécessaire, tenues à jour ; toutes les mesures raisonnables doivent être prises pour que les données à caractère personnel qui sont inexactes, eu égard aux finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans tarder ;

e) conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées ;

f) traitées de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées (intégrité et confidentialité) ; »[139]

De cette manière, le recueil et l'exploitation par les journalistes des données à partir de l'Open Source est règlementé quant à la manière dont les données doivent être collectées dans un but précis appelé « finalité » c'est-à-dire qu'il doit tendre vers un objectif légitime, et donc ne doivent pas être récoltées au détriment de la vie privée de la personne concernée.

Le traitement de ces données doit être effectué dans un principe de respect des données (licite, loyal et transparent). La transparence est d'ores et déjà utilisées par les sociétés de

[139] CNIL, « Chapitre II – Principes », 23 mai 2018, https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre2#Article11

journalisme qui partagent les étapes de leurs enquêtes lorsqu'elles sont effectuées en open source.

L'exigence d'exactitude quant à elle vise à obliger l'utilisateur à effectuer un travail de rechercher pour lutter contre la diffamation. De plus, leur conservation est limitée dans le temps pour s'assurer que les données ne seront pas utilisées ultérieurement pour l'accomplissement d'autres finalités étrangères à celles prévues initialement.

L'analyse d'impact. Lorsqu'un traitement a la possibilité d'engendrer un risque important d'atteinte aux droits et libertés des individus, le responsable de traitement a désormais l'obligation de réaliser une analyse d'impact pour évaluer « l'origine, la nature, la particularité et la gravité de ce risque » selon l'article juridique « Données personnelles et sécurité » de Christiane Féral-Schuhl.

Selon elle « l'analyse d'impact doit (i) décrire les opérations de traitement et les finalités, y compris, le cas échéant, l'intérêt légitime poursuivi par le responsable du traitement; (ii) évaluer la nécessité et la proportionnalité des opérations de traitement au regard de la finalité, (iii) évaluer les risques pour les droits et libertés des personnes concernées ainsi que (iv) les mesures envisagées pour faire face aux risques, y compris les garanties, mesures et mécanismes de sécurité visant à assurer la protection des données à caractère personnel et à apporter la preuve du respect du présent règlement, compte tenu des droits et des intérêts légitimes des personnes concernées et des autres personnes affectées ».

En fonction des résultats de l'analyse, des mesures adéquates devront être prises par le responsable de traitement dans le but de limiter ce risque tels que l'anonymisation ou « pseudonymisation », la réduction du volume de données traitées ou encore l'imposition de délai pour l'effacement des données. Dans le cas où les risques ne peuvent pas être diminués, en raison des techniques accessibles et de leurs coûts, l'autorité de contrôle devra être consultée préalablement au traitement. Elle disposera alors, toujours selon l'auteur, de tous les pouvoirs tels qu'ils sont prévus à l'article 58 du règlement 2016/679 : de pouvoirs d'adopter des mesures correctrices, d'enquête par exemple.

De cette façon, le RGPD couvre d'ores et déjà de façon certaines le respect des libertés individuelles. Des protections sont prévues pour les situations où les risques d'atteintes sont envisageables permettant ainsi de les faire disparaitre.

Aujourd'hui, il n'existe pas encore de législation spécifique consacrée aux réseaux sociaux mais ils sont tout de même soumis au droit commun. Ainsi, bien que le RGPD ne s'applique pas aux traitements de données à caractère personnel lorsque ceux-ci sont effectués au cours d'activités strictement personnelles ou domestiques[140], il « s'applique aux responsables du traitement ou aux sous-traitants qui fournissent les moyens de traiter des données à caractère personnel pour de telles activités personnelles ou domestiques ».

De cette manière, bien qu'un droit régissant spécifiquement l'utilisation des réseaux n'existe pas encore, le RGPD protège les données personnelles en fonction de leur utilisation de façon plus général sur internet ainsi que de l'usage qui en sera fait. Il règlemente plus particulièrement les sociétés privées et a pour vocation plus particulièrement d'ériger un rempart vis-à-vis du GAFAM.

Le GAFAM est un acronyme qui désigne ce qu'on appelle aujourd'hui les « géants de la technologie que sont Google, Apple, Facebook, Amazon et Microsoft. Ce sont les cinq entreprises américaines du secteur de la technologie qui sont les plus influents et côtés en bourse. Les avancées technologiques ont favorisé la numérisation de notre quotidien dont le secteur est contrôlé par cette poignée d'acteurs. Ils rivalisent sur plusieurs marchés comme les systèmes d'exploitation pour mobile et ordinateur portable, le matériel informatique et enfin le divertissement. Ils entrent désormais en concurrence dans des domaines dont les technologies numériques sont plus avancées à l'image de l'intelligence artificielle et du cloud.

Il apparait alors que le RGPD a pour vocation initiale de défendre les données à caractère personnel des individus contre le GAFAM qui récolte et exploite ces dernières dans un but purement commercial.

[140] Le RGPD affirme que « les activités personnelles ou domestiques pourraient inclure l'échange de correspondance et la tenue d'un carnet d'adresses, ou l'utilisation de réseaux sociaux et les activités en ligne qui ont lieu dans le cadre de ces activités »

§2 Des évolutions envisagées

La présidente de la CNIL, lors du rapport annuel de la CNIL, « le bilan 2021 de la CNIL témoigne d'une activité particulièrement intense, marquée par une politique d'accompagnement renouvelée, l'accroissement des mesures répressives et un renforcement des actions pour la cybersécurité »[141].

Elle ajoute que « Plus que jamais, c'est le respect d'un équilibre entre accompagnement de la transformation numérique et protection des droits des personnes qui permettra de relever les défis soulevés par la numérisation de notre environnement quotidien ».

En effet, l'anticipation et l'innovation font partie des missions essentielles de la CNIL. Les débats de sociétés pour les enjeux éthiques des données auxquels elle contribue représente une rencontre avec les différents domaines d'innovation du numérique que sont les chercheurs, les laboratoires et les start-ups. De cette manière, elle contribue au développement des technologies protectrices de la vie privée.

Le développement rapide de l'intelligence artificielle conduit à mettre certains principes du RGPD et de la loi informatique et libertés en difficulté. C'est pourquoi la CNIL mène plusieurs travaux dont le but est de préciser la manière d'assurer la conformité des traitements de données qui recourent à ces systèmes tout en prenant part aux discussions sur le futur règlement européen consacré à l'IA en cours d'élaboration.

La CNIL a prévu un nouveau plan stratégique 2022-2024 pour une société numérique de confiance. Pour se faire, il s'articule autour de 3 axes : favoriser le respect des droits, promouvoir le RGPD comme un atout et enfin cibler la régulation sur des sujets primordiaux[142].

De cette manière, la CNIL souhaite favoriser la maitrise et le respect des droits des personnes sur le terrain. Dans cette optique, quatre objectifs ont été fixés que sont le renforcement de l'information et la sensibilisation des personnes pour favoriser l'exercice des droits, l'accroissement de l'efficacité de l'action répressive., le renforcement du rôle européen de la CNIL et l'efficacité du collectif européen et enfin la priorisation des actions pour protéger les usages du quotidien.

---

[141] CNIL, « Rapport annuel : Commission nationale de l'informatique et des libertés », 2021, https://www.cnil.fr/sites/default/files/atoms/files/cnil_-_42e_rapport_annuel_-_2021.pdf

[142] Bis 135

Le second axe concerne donc la volonté de promouvoir le RGPD comme atout de confiance pour les responsables de traitement. La CNIL prévoit encore de « renforcer son offre d'accompagnement en facilitant la compréhension et la prévisibilité du cadre légal, en développant des outils de conformité et en les aidant à se pré- munir contre les risques cyber.

Elle fera également évoluer sa stratégie d'accompagnement grâce à de nouveaux outils de type « bac à sable ». Au-delà d'une culture de conformité et de ses avantages, elle agira pour que les acteurs publics et privés se saisissent du RGPD comme d'un atout pour leur image ou leur compétitivité. »

Le troisième axe à évaluer les priorités vis-à-vis de l'intensification des usages des données personnelles. Pour cela, trois thématiques ont été retenues : tout d'abord face au développement massif des caméras « augmentées » sur le terrain qui sont souvent accompagnées de logiciel prédictifs il est primordial d'évaluer leur caractère nécessaire et proportionné qui présente un risque : la surveillance à grande échelle.

Ensuite, le plan d'action de la CNIL concernant le transfert de données dans l'informatique en nuage[143], « en coopération avec ses homologues européens, permettra, sur le fondement de l'arrêt dit « Schrems II », de sécuriser les transferts de données personnelles des Français vers des pays en dehors de l'Union européenne ».

En dernier lieu, face à la collecte massive de données personnelles par le biais des applications mobiles, la CNIL prévoit de « rendre visibles les flux de données et renforcer la conformité des applications mobiles et de leurs écosystèmes, pour mieux protéger la vie privée des utilisateurs d'ordiphones (smartphones) »[144].

En 2022, le Laboratoire d'Innovation Numérique de la CNIL (LINC) ainsi à la chaîne de la donnée captée par le biais de ces applications. Tout d'abord, il étudiera des outils permettant d'analyser des applications puis la diffusion et la revente des données collectées depuis ces dernières. C'est une étude qui permettra de mettre en lumière la chaîne de la donnée, de la collecte à sa réutilisation. Le LINC poursuivra également l'étude des « dark patterns » en analysant les bandeaux cookies qui influent sur le choix des utilisateurs.

[143] Les applications et les données ne se trouvent plus sur un ordinateur déterminé mais dans un nuage (cloud) composé de nombreux serveurs distants interconnectés selon la CNIL.
[144] Idem 136

Conclusion

Les avancées technologiques nous permettent d'innover pour rendre la vie quotidienne plus simple, se rendre plus compétitifs à l'international mais aussi de développer des domaines très variés comme celui de la santé, de l'économie, de l'éduction ou encore de la géopolitique.

Cependant, si elles reflètent les avancées positives, plus les technologies numériques se développent, plus les enjeux de cette évolution et ses défis augmentent de façon corolaire. Le droit est le domaine le plus impacté parce qu'il doit sans cesse créé des normes, réformer, adapter ses règles juridiques au gré de ce développement. Chaque innovation donne lieu à l'apparition de vide législatif au départ et nécessite des longues réflexions dans le but d'évaluer la proportionnalité entre la norme envisagée et le respect des droits et libertés individuelles.

La délinquance a changé de forme ces dernières années, le numérique augmentant considérablement le champ infractionnel disponible. L'arrivée d'Internet et le développement du web et des réseaux sociaux qui ont entrainé une scission entre la réalité et le virtuel. En effet, il existe désormais deux types de relationnel : les interactions des individus lorsqu'ils se rencontrent physiquement et celles des internautes qui communiquent par le biais d'un réseau de télécommunication c'est-à-dire par un échange de données.

Les enquêteurs rencontrent des difficultés dans la conduite des investigations tant au stade de la recherche de preuves numériques qui nécessitent une habilitation et des connaissances pointues dans le fonctionnement des outils numériques. Mais l'ère du numérique offre aussi aux forces de police de nouvelles façons plus rapides et efficaces de mener ces investigations.

Quand bien même les enquêteurs auront sans doute toujours besoin de s'appuyer sur des preuves matérielles et sur leurs techniques d'enquête et d'interrogatoire pour résoudre un crime, l'examen des preuves numériques occupe une part toujours plus grande du processus, sachant que les traces numériques reflètent plus ce qu'est une personne dans notre monde d'aujourd'hui.

Tel est le cas de la vidéoprotection combinée à des logiciels de reconnaissance faciale, les drones qui permettent de mettre en place des systèmes de surveillance pilotés à distance.

C’est aussi le cas désormais de logiciels dits « prédictifs » basés sur l’intelligence artificielle, permettant de prévoir le lieu et l’endroit où un crime est le plus susceptible de se commettre. Le recours aux logiciels de centralisation est aussi un atout important de sécurité combinant le regroupement national des fichiers que la police possède avec des logiciels de reconnaissance facial.

Ainsi, l’adaptation des outils à la disposition des enquêteurs est devenue un enjeu primordial dans notre société actuelle. Aujourd’hui, l’Etat en a pris conscience et se lance dans une course à l’innovation mais à quel prix ?

Si on n’intègre pas de nouveaux moyens d’enquêtes, il sera impossible pour l’Etat de garantir une sécurité collective à l’avenir. Pourtant l’intégration de technologies performantes engendre de plus en plus d’atteintes aux droits et libertés fondamentaux. L’enjeu d’aujourd’hui n’est donc plus de savoir quels outils assimiler aux moyens d’investigations mis comment effectuer la balance entre sécurité et liberté ?

Une balance qui, en France, est confiée au Conseil constitutionnel. Ce défi trouve son illustration dans la quantité importante de lois censurées par le Conseil lors de son contrôle a priori. Le législateur peine à trouver cet équilibre précaire car les technologies modernes sont, à l’image de la reconnaissance faciale, par définition plus attentatoires que les précédentes.

Plus précisément, l’accès et la conservation de données à caractère personnel est nécessaire au fonctionnement correct de ces logiciels. Elle récolte le nom, le prénom et l’image du visage de l’individu, autant de caractéristiques qui sont au cœur de la vie privée des individus. Les dispositifs aéroportés quant à eux peuvent désormais capter des images et sons à des distances importantes sans que la personne surveillée ne soit alertée. Ces appareils peuvent se déplacer sur de longues distances ce qui signifie qu’il est possible de suivre une personne sans interruption pour collecter des informations telles que sur ses convictions religieuses, sa vie familiale et sentimentale, ses activités en dehors de son travail etc.

Avec les avancées scientifiques, les logiciels d’intelligence artificielle sont régulièrement testés et présentent des failles au sien de leur programmation comme les biais cognitif, brouillant la perception objective initialement souhaitée par points de vue discriminatoire voir politiquement orientée. Aujourd’hui, ces outils reflètent de façon plutôt exacte les prévisions des œuvres anciennes telles que Big Brother dont la description de Georges Orwell rappelle les expériences menées en Chine.

Ces constations sont pour le moins alertant concernant les utilisations futures de l'IA. C'est pour cette raison que de nombreux projets sont en cours, dont l'objectif est d'encadrer spécifiquement l'IA et de tenter de prévenir les risques subséquents qu'engendrerait leur utilisation à grande échelle.

Mais les dangers n'en restent pas là. Les citoyens participent dorénavant au processus de lutte contre la délinquance. Autrefois le domaine exclusif de la police étatique, les personnes privées exploitent maintenant les outils numériques à leur libre disposition pour enquêter et mettre à jour l'existence de certaines infractions inconnues ou pas suffisamment identifiées par les forces de police.

Deux types de pratiques se sont alors développées : l'Open Source Intelligente et les milices numériques. La première a fait ses preuves lorsque les sociétés de journalisme, par un travail d'investigation novateur, ont permis d'apporter les preuves suffisantes pour élucider le meurtre de deux femmes et deux enfants au Cameroun est identifier les auteurs. De plus, l'Open Source a été un atout majeur depuis le début de la guerre en Ukraine, valorisant une nouvelle utilisation : la prévision des attaques ennemies et l'élaboration de stratégies adaptées en tant de guerre.

La deuxième est apparu par le rassemblement de personnes possédant des histoires semblables résultant d'infractions particulières. Tel a été le cas des milices apparues dans le cadre de la lutte contre la pédopornographie et contre les violences sexuelles. Chaque protagoniste ayant permis le développement de ce phénomène était soit victime soit le proche de l'une d'elles. Mobilisés autour de valeurs communes, ces citoyens ont donné lieu à la libération de la parole des femmes sur ces violences ainsi que la mise en lumière de très nombreux cas de pédopornographie par le biais des réseaux sociaux.

Cependant, ces différentes enquêtes citoyennes ne sont pas prévues par la loi et, les données étant accessibles librement et gratuitement, de ce fait relèvent du droit commun. Le RGPD est un texte très important qui règlemente la collecte et l'utilisation des données à caractère personnel par les plateformes numériques. Il a initié la règlementation à grande échelle des données numériques dites « à caractère personnel »

Nous sommes à l'aune d'une nouvelle ère, les personnes privées ayant initié un travail d'investigations en parallèle des enquêteurs pour lutter contre la désinformation des Etats. Aujourd'hui, il n'est pas profitable de mettre un terme aux enquêtes citoyennes, d'une part, elles ne font qu'exploiter des données accessibles par tous mais d'autre part elles ont prouvé l'apport bénéfiques qu'elles pouvaient procurer aux enquêteurs étatiques.

Une chose est sûre, le législateur va intervenir pour réguler ce phénomène mais de quelle manière ? La possibilité d'une coopération entre les personnes privées et les autorités publique pourrait perfectionner les techniques préexistantes mais aussi révolutionner la lutte contre la délinquance en apportant un regard neuf sur ces techniques.

Cependant, une telle collaboration doit être strictement encadrée, il n'est pas question que les citoyens puissent accéder aux fichiers des services de police. Leur collaboration devra être limitée mais aura peut-être pour avantage de pallier le manque d'effectifs dont pâtissent les enquêteurs.

A l'échelle internationale, les risques de l'évolution vers une société de surveillance ce sont d'ores et déjà illustrée par l'intermédiaire des régimes politique de Chine et de Russie. L'oppression d'une minorité par l'installation massive de caméras mais aussi la création du système de crédit social et l'emploi massif de la reconnaissance faciale à l'heure actuelle présage un futur plus sombre encore. De quelle manière vont évoluer ces régimes politiques avec le développement de l'IA ? Si ces pays poursuivent leur cheminement dans l'utilisation des technologies numériques modernes pour contrôler la population, qu'en sera-t-il lorsque les dispositifs d'IA possèderont des capacités d'intelligence à l'image de l'homme ? Il n'existe pas encore de réponse à ces interrogations, mais une chose est sûre, les atteintes aux droits et libertés fondamentaux vont être de plus en plus graves.

Bibliographie

Articles Internet

Arthur Le Denn, « La police de Los Angeles abandonne PredPol, le logiciel qui prédit les crimes », 2020, https://www.usine-digitale.fr/article/la-police-de-los-angeles-abandonne-predpol-le-logiciel-qui-predit-les-crimes.N956926

Albane Dreyer, « L'investigation numérique, révolution de la pratique journalistique », 2021 https://www.mesdatasetmoi-observatoire.fr/article/linvestigation-numerique-revolution-de-la-pratique-journalistique

Assemblée Nationale, Déclaration des Droits de l'Homme et du Citoyen de 1789, 1798 https://www.legifrance.gouv.fr/contenu/menu/droit-national-en-vigueur/constitution/declaration-des-droits-de-l-homme-et-du-citoyen-de-1789

BBC News, Anatomy of a Killing, 2018, https://www.youtube.com/watch?v=4G9S-eoLgX4

Bruno Le Maire, Frédérique Vidal et Cédric O, « Stratégie nationale pour l'intelligence artificielle – 2e phase : Conquérir les talents et transformer notre potentiel scientifique en succès économiques », 2021, https://minefi.hosting.augure.com/Augure_Minefi/r/ContenuEnLigne/Download?id=334FD34F-7844-497E-9551-79EDFF3B2EEF&filename=1645%20-%20DP%20-%20Strat%C3%A9gie%20Nationale%20pour%20l%27IA%202%C3%A8me%20phase.pdf

Clarisse Serre et Charles Evrard, « Du rififi chez les grandes oreilles », 2020, https://www.dalloz-actualite.fr/node/du-rififi-chez-grandes-oreilles

CNIL, « Biométrie », https://www.cnil.fr/fr/definition/biometrie
Thales, « La biométrie au service de l'identification et l'authentification », 2021, https://www.thalesgroup.com/fr/europe/france/dis/gouvernement/inspiration/biometrie

CNIL, « Chapitre I - Dispositions générales », https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre1#Article1

CNIL, « Chapitre II – Principes », 23 mai 2018, https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre2#Article11

CNIL, « FAED : Fichier automatisé des empreintes digitales », 2018, https://www.cnil.fr/fr/faed-fichier-automatise-des-empreintes-digitales

CNIL, « FNAEG : Fichier national des empreintes génétiques », 2018, https://www.cnil.fr/fr/fnaeg-fichier-national-des-empreintes-genetiques

CNIL, « Mission 3 - Anticiper et innover », https://www.cnil.fr/fr/mission-de-la-CNIL-anticiper-innovation

CNIL, « TAJ : Traitement d'Antécédents Judiciaires », 2018, https://www.cnil.fr/fr/taj-traitement-dantecedents-judiciaires

Constance Le Grip, 15ème législature Question N° 3287, 2017-2018, https://questions.assemblee-nationale.fr/q15/15-3287QE.htm

CNIL, « Rapport annuel : Commission nationale de l'informatique et des libertés », 2021, https://www.cnil.fr/sites/default/files/atoms/files/cnil_-_42e_rapport_annuel_-_2021.pdf

CNIL, « RGPD : de quoi parle-t-on ? », https://www.cnil.fr/fr/rgpd-de-quoi-parle-t-on

Gérald DARMANIN, « Projet de loi nº 5185 d'orientation et de programmation du ministère de l'intérieur », 2022, https://www.assemblee-nationale.fr/dyn/15/textes/l15b5185_projet-loi#

Commission européenne, « L'Alliance européenne de l'IA, 2022 », https://digital-strategy.ec.europa.eu/fr/policies/european-ai-alliance

CNIL, « Mission 4 - Contrôler et sanctionner », https://www.cnil.fr/fr/mission-4-controler-et-sanctionner

Commission Européenne, « Intelligence artificielle : la Commission franchit une étape dans ses travaux sur les lignes directrices en matière d'éthique », 2019, https://ec.europa.eu/commission/presscorner/detail/fr/IP_19_1893

Cyrille Chausson, Définition Open Source, 2016, https://www.lemagit.fr/definition/Open-Source

Deveryware, « La data au cœur de l'enquête », Livre blanc, octobre 2020

Devrum, « Comparaison entre l'intelligence artificielle et le Big Data », 13 juin 2018, http://blog.devrun.com/l-article/comparaison-entre-l-intelligence-artificielle-et-le-big-data

Direction des affaires juridiques, « Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés », 06 janvier 1978 http://affairesjuridiques.aphp.fr/textes/loi-n-78-17-du-6-janvier-1978-relative-a-linformatique-aux-fichiers-et-aux-libertes/

Dorian De Schaepmeester, « Comment l'open source intelligence est devenue une arme majeure dans la guerre en Ukraine ? », 2022, https://www.futura-sciences.com/tech/actualites/guerre-futur-crimes-guerre-ukraine-ces-francais-traquent-preuves-98366/

Eric OK, « La preuve numérique, Un défi pour l'enquête criminelle du 21e siècle », Les cahiers du numérique, https://www.cairn.info/revue-les-cahiers-du-numerique-2003-3-page-205.htm

Faustine Vincent, « Comment la BBC a retrouvé le lieu et la date d'exécutions filmées au Cameroun », 2018, https://www.lemonde.fr/big-browser/article/2018/09/27/executions-filmees-au-cameroun-la-prouesse-journalistique-de-la-bbc_5360895_4832693.html

François Pellegrini, Sébastien Canevet, « Le droit du numérique : une histoire à préserver », 2013 https://edutice.archives-ouvertes.fr/edutice-00940669/file/a1311e.htm

Frédéric Durand, « En Normandie, les « chasseurs de pédophiles » enquêtent, les autorités se méfient », 2020, https://www.leparisien.fr/faits-divers/en-normandie-les-chasseurs-de-pedophiles-enquetent-les-autorites-se-mefient-23-09-2020-8389875.php

Jean-Baptiste Thomas-Sertillanges, « Droit et technologies : concilier l'inconciliable ? », *Réflexions épistémologiques pour un droit des libertés technologiques, Les Cahiers du numérique*, 2014, https://www.cairn.info/revue-les-cahiers-du-numerique-2014-2-page-17.htm

Julien BONNET, Pauline TÜRK, « Nouveaux Cahiers du Conseil constitutionnel n° 57 (dossier : droit constitutionnel à l'épreuve du numérique) », 2017, https://www.conseil-constitutionnel.fr/nouveaux-cahiers-du-conseil-constitutionnel/le-numerique-un-defi-pour-le-droit-constitutionnel

Julien Bonnet et Pauline Türk, « Le numérique : un défi pour le droit constitutionnel », 2017, https://www.conseil-constitutionnel.fr/nouveaux-cahiers-du-conseil-constitutionnel/le-numerique-un-defi-pour-le-droit-constitutionnel

Larousse, Définition technologie, https://www.larousse.fr/dictionnaires/francais/technologie/76961

« Le groupe Deveryware », 2020, https://www.tracip.fr/le-groupe-deveryware

Le groupe Deveryware, « Le Groupe Deveryware publie son livre blanc « La Data au cœur de l'enquête », 2020, https://www.tracip.fr/le-groupe-deveryware/

Les Observateurs, « Les observateurs France 24, Enquête vidéo : Iran, massacre à huis clos », 2020, https://observers.france24.com/fr/20200110-enquete-video-iran-massacre-manifestations-internet

Louis Dumestre, « Éthique et Intelligence Artificielle : l'expérience « Morale Machine » », 2020, https://portail-ie.fr/analysis/2371/ethique-et-intelligence-artificielle-lexperience-morale-machine

Ministère de la Justice, « Informatique et libertés : Plate-forme nationale des interceptions judiciaires », 2022, https://www.justice.fr/donnees-personnelles/PNIJ

Marcello Vitali-Rosati, Pour une définition du « numérique », https://louisderrac.com/wp-content/uploads/2019/09/Pour-une-definition-du-numerique_Vitali-Rosati.pdf
Morgan Tual, « Polémique sur une étude affirmant qu'un programme peut repérer l'homosexualité sur le visage », 2017 https://www.lemonde.fr/pixels/article/2017/09/12/polemique-apres-une-etude-affirmant-qu-un-programme-peut-reperer-l-homosexualite-sur-le-visage_5184516_4408996.html

Marc Zaffagni, « Crimes de guerre en Ukraine : ces Français traquent les preuves », 2022, https://www.futura-sciences.com/tech/actualites/guerre-futur-crimes-guerre-ukraine-ces-francais-traquent-preuves-98366/

Ministère de l'économie, des finances et de la souveraineté industrielle et numérique, La stratégie nationale pour l'intelligence artificielle, 2021, https://www.economie.gouv.fr/strategie-nationale-intelligence-artificielle

Ministère de l'intérieur, « Projet de loi d'orientation et de programmation du ministère de l'intérieur 2022-2027 », 2022, https://www.interieur.gouv.fr/sites/minint/files/medias/documents/2022-03/16-03-2022-projet-de-loi-d-orientation-et-de-programmation-du-ministere.pdf

Murielle Cahen, « Les risques juridiques des logiciels de reconnaissance FACIALE », 2021,

https://www.murielle-cahen.com/publications/reconnaissance%20-faciale.asp

Octets de Vie, Exemples de technologie numérique et sa définition, https://vidabytes.com/fr/ejemplos-de-tecnologia-digital/#Definiendo_tecnologia_digital
Serge Braudo, Définition de NTIC (nouvelles technologies de l'information et de la communication), https://www.dictionnaire-juridique.com/definition/ntic-nouvelles-technologies-de-l-information-et-de-la-communication.php

Parlement européen, « Règlementation de la reconnaissance faciale au sein de l'Union européenne », 2021, https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/698021/EPRS_IDA(2021)698021_FR.pdf

Philippe Rioux, « Les nouvelles techniques d'enquête », 2017, https://www.ladepeche.fr/article/2017/06/17/2595775-les-nouvelles-techniques-d-enquete.html
Pôle Judiciaire de la Gendarmerie Nationale, « Les traces papillaires ensanglantées »,

https://www.gendarmerie.interieur.gouv.fr/pjgn/ircgn/l-expertise-

decodee/identification/les-traces-papillaires-ensanglantees

Pôle Judicaire de la Gendarmerie Nationale, Les cyber-enquêteurs alertent sur les difficultés levées par les «chasseurs de pédophiles», https://www.gendarmerie.interieur.gouv.fr/pjgn/actualite/vu-dans-les-medias/les-cyber-enqueteurs-alertent-sur-les-difficultes-levees-par-les-chasseurs-de-pedophiles

Simon Petite, « Bellingcat, le site qui aligne les révélations sur l'affaire Skripal », 2018 https://www.letemps.ch/monde/bellingcat-site-aligne-revelations-laffaire-skripal

Ouvrages

Basile Thodoroff, Arno Amabile, *Police numérique, une révolution sous surveillance* ?, Ecole des Mines, 2020
George Orwell, *1984*, Secker and Warburg, 8 juin 1949

Olivier Aim « Les théories de la surveillance - Du panoptique aux Surveillance Studies », *Armand Colin*, 2020

Articles

Céline Castets-Renard, « L'IA en pratique : la police prédictive aux États-Unis », Dalloz IP/IT, 2019, https://www-dalloz-fr.lama.univ-amu.fr/documentation/Document?ctxt=0_YSR0MD1wb2xpY2UgcHLDqWRpY3RpdmUgw6l0YXRzIHVuaXPCp3gkc2Y9c2ltcGxlLXNlYXJjaA%3D%3D&ctxtl=0_cyRwYWdlTnVtPTHCp3MkdHJpZGF0ZT1GYWxzZcKncyRzb3J0PSNkZWZhdWx0X0Rlc2PCp3Mkc2xOYlBhZz0yMMKncyRpc2Fibz1UcnVlwqdzJHBhZ2luZz1UcnVlwqdzJG9uZ2xldD3Cp3MkZnJlZXNjb3BlPUZhbHNlwqdzJHdvSVM9RmFsc2XCp3Mkd29TUENIPUZhbHNlwqdzJGZsb3dNb2RlPUZhbHNlwqdzJGJxPcKncyRzZWFyY2hMYWJlbD3Cp3Mkc2VhcmNoQ2xhc3M9&id=DIPIT%2FCHRON%2F2019%2F0234

Christiane Féral-Schuhl, , « Chapitre 712 - Atteintes aux systèmes d'information », *Praxis Cyberdroit*, 2020-2021, https://www-dalloz-fr.lama.univ-amu.fr/documentation/Document?id=DZ%2FPRAXIS%2FCYBERDROIT%2F2019%2FL07-T71-C712%2FPLAN%2F0010&ctxt=0_YSR0MD1mYWtlIG5ld3PCp3gkc2Y9c2ltcGxlLXNlYXJjaA%3D%3D&ctxtl=0_cyRwYWdlTnVtPTHCp3MkdHJpZGF0ZT1GYWxzZcKncyRzb3J0PSNkZWZhdWx0X0Rlc2PCp3Mkc2xOYlBhZz0yMMKncyRpc2Fibz1UcnVlwqdzJHBhZ2luZz1UcnVlwqdzJG9uZ2xldD3Cp3MkZnJlZXNjb3BlPUZhbHNlwqdzJHdvSVM9RmFsc2XCp3Mkd29TUENIPUZhbHNlwqdzJGZsb3dNb2RlPUZhbHNlwqdzJGJxPcKncyRzZWFyY2hMYWJlbD3Cp3Mkc2VhcmNoQ2xhc3M9&scrll=DZ%2FPRAXIS%2FCYBERDROIT%2F2019%2FPARA%2F712.101

Christiane Féral-Schuhl, « Les enquêtes dans l'environnement numérique », *Praxis Cyberdroit*, 2020-2021, Titre 72, https://www-dalloz-fr.lama.univ-amu.fr/documentation/Document?id=DZ%2FPRAXIS%2FCYBERDROIT%2F2019%2FNIVO%2FL07-T72&ctxt=0_YSR0MD1iaWcgZGF0YSBldCBlbnF1w6p0ZXMgZGUgcG9saWNlwqd4JHNmPXNpbXBsZS1zZWFyY2g%3D&ctxtl=0_cyRwYWdlTnVtPTHCp3MkdHJpZGF0ZT1GYWxzZcKncyRzb3J0PSNkZWZhdWx0X0Rlc2PCp3Mkc2xOYlBhZz0yMMKncyRpc2Fibz1UcnVlwqdzJHBhZ2luZz1UcnVlwqdzJG9uZ2xldD3Cp3MkZnJlZXNjb3BlPUZhbHNlwqdzJHdvSVM9RmFsc2XCp3Mkd29TUENIPUZhbHNlwqdzJGZsb3dNb2RlPUZhbHNlwqdzJGJxPcKncyRzZWFyY2hMYWJlbD3Cp3Mkc2VhcmNoQ2xhc3M9&scrll=ANOTE_DZ%2FPRAXIS%2FCYBERDROIT%2F2019%2FPARA%2F72.05_1

Frédérique CHOPIN, « Cybercriminalité », *Répertoire IP/IT et Communication*, Dalloz, 2020 https://www-dalloz-fr.lama.univ-amu.fr/documentation/Document?id=ENCY%2FIPIT%2FPENRUB000083&ctxt=0_YSR0MD1jeWJlcmNyaW1pbmFsaXTDqcKneCRzZj1zaW1wbGUtc2VhcmNo&ctxtl=0_cyRwYWdlTnVtPTHCp3MkdHJpZGF0ZT1GYWxzZcKncyRzb3J0PSNkZWZhdWx0X0Rlc2PCp3Mkc2xOYlBhZz0yMMKncyRpc2Fibz1UcnVlwqdzJHBhZ2luZz1UcnVlwqdzJG9uZ2xldD3Cp3MkZnJlZXNjb3BlPUZhbHNlwqdzJHdvSVM9RmFsc2XCp3Mkd29TUENIPUZhbHNlwqdzJGZsb3dNb2RlP

UZhbHNlwqdzJGJxPcKncyRzZWFyY2hMYWJlbD3Cp3Mkc2VhcmNoQ2xhc3M9&scrll=ENCY%2FIPIT%2FPENRUB000083%2F2020-02%2FPARA%2F7

Gérard HAAS, Stéphane ASTIER, « Les biais de l'intelligence artificielle : quels enjeux juridiques ? » *Répertoire IP/IT et Communication*, 2019, https://www-dalloz-fr.lama.univ-amu.fr/documentation/Document?id=ENCY%2FIPIT%2FRUB000429&ctxt=0_YSR0MD1Hw6lyYXJkIEhBQVMsIFN0w6lwaGFuZSBBU1RJRVIgTGVzIGJpYWlzIGRlIGwnaW50ZWxsaWdlbmNlIGFydGlmaWNpZWxsZSA6IHF1ZWxzIGVuamV1eCBqdXJpZGlxdWVzIMKneCRzZj1zaW1wbGUtc2VhcmNo&ctxtl=0_cyRwYWdlTnVtPTHCp3MkdHJpZGF0ZT1GYWxzZcKncyRzb3J0PSNkZWZhdWx0X0Rlc2PCp3Mkc2xOYlBhZz0yMMKncyRpc2Fibz1UcnVlwqdzJHBhZ2luZz1UcnVlwqdzJG9uZ2xldD3Cp3MkZnJlZXNjb3BlPUZhbHNlwqdzJHdvSVM9RmFsc2XCp3Mkd29TUENIPUZhbHNlwqdzJGZsb3dNb2RlPUZhbHNlwqdzJGJxPcKncyRzZWFyY2hMYWJlbD3Cp3Mkc2VhcmNoQ2xhc3M9&scrll=ENCY%2FIPIT%2FRUB000429%2F2019-09%2FSOMMAIRE

Marc Schwendenert, « Police technique et scientifique », *Répertoire de droit pénal et de procédure pénale*, 2016, https://www-dalloz-fr.lama.univ-amu.fr/documentation/Document?ctxt=0_YSR0MD1Qb2xpY2UgdGVjaG5pcXVlIGV0IHNjaWVudGlmaXF1ZSDCp3gkc2Y9c2ltcGxlLXNlYXJjaA%3D%3D&ctxtl=0_cyRwYWdlTnVtPTHCp3MkdHJpZGF0ZT1GYWxzZcKncyRzb3J0PSNkZWZhdWx0X0Rlc2PCp3Mkc2xOYlBhZz0yMMKncyRpc2Fibz1UcnVlwqdzJHBhZ2luZz1UcnVlwqdzJG9uZ2xldD3Cp3MkZnJlZXNjb3BlPUZhbHNlwqdzJHdvSVM9RmFsc2XCp3Mkd29TUENIPUZhbHNlwqdzJGZsb3dNb2RlPUZhbHNlwqdzJGJxPcKncyRzZWFyY2hMYWJlbD3Cp3Mkc2VhcmNoQ2xhc3M9&id=ENCY%2FPEN%2FRUB000387

Gérard Haas, « La cybercriminalité à la fois côté obscur et face cachée du Big Data », Dalloz, 2016, p.21, https://www-dalloz-fr.lama.univ-amu.fr/documentation/Document?id=DIPIT%2FCHRON%2F2015%2F0041&ctxt=0_YSR0MD1iaWcgZGF0YcKneCRzZj1zaW1wbGUtc2VhcmNo&ctxtl=0_cyRwYWdlTnVtPTHCp3MkdHJpZGF0ZT1GYWxzZcKncyRzb3J0PSNkZWZhdWx0X0Rlc2PCp3Mkc2xOYlBhZz0yMMKncyRpc2Fibz1UcnVlwqdzJHBhZ2luZz1UcnVlwqdzJG9uZ2xldD3Cp3MkZnJlZXNjb3BlPUZhbHNlwqdzJHdvSVM9RmFsc2XCp3Mkd29TUENIPUZhbHNlwqdzJGZsb3dNb2RlPUZhbHNlwqdzJGJxPcKncyRzZWFyY2hMYWJlbD3Cp3Mkc2VhcmNoQ2xhc3M9

Yves Mayaud, « Terrorisme – Poursuites et indemnisation », *Répertoire de droit pénal et de procédure pénale*, 2020, https://www-dalloz-fr.lama.univ-amu.fr/documentation/Document?id=ENCY%2FPEN%2FRUB000396%2F2020-02%2FPARA%2F272&ctxt=0_YSR0MD10ZWNobmlxdWVzIHNww6ljaWFsZXMgZCdlbnF1w6p0ZcKneCRzZj1zaW1wbGUtc2VhcmNo&ctxtl=0_cyRwYWdlTnVtPTHCp3MkdHJpZGF0ZT1GYWxzZcKncyRzb3J0PSNkZWZhdWx0X0Rlc2PCp3Mkc2xOYlBhZz0yMMKncyRpc2Fibz1UcnVlwqdzJHBhZ2luZz1UcnVlwqdzJG9uZ2xldD3Cp3MkZnJlZXNjb3BlPUZhbHNlwqdzJHdvSVM9RmFsc2XCp3Mkd29TUENIPUZhbHNlwqdzJGZsb3dNb2RlPUZhbHNlwqdzJGJxPcKncyRzZWFyY2hMYWJlbD3Cp3Mkc2VhcmNoQ2xhc3M9&scrll=ENCY%2FPEN%2FRUB000396%2F2020-02%2FPARA%2F273

Philippe le Tourneau, , « Chapitre 221 - Qualification du logiciel », *Dalloz référence Contrats du numérique*, Dalloz, 2021-2022, https://www-dalloz-fr.lama.univ-amu.fr/documentation/Document?id=DZ%2FREFERENCE%2FCONTRATS-NUMERIQUE%2F2020%2FL02-T22-C221%2FPLAN%2F0002&ctxt=0_YSR0MD1vcGVuIHNvdXJjZSBpbnRlbGxpZ2VuY2XCp3gkc2Y9c2ltcGxlLXNlYXJjaA%3D%3D&ctxtl=0_cyRwYWdlTnVtPTHCp3MkdHJpZGF0ZT1GYWxzZcKncyRzb3J0PSNkZWZhdWx0X0Rlc2PCp3Mkc2xOYlBhZz0yMMKncyRpc2Fibz1UcnVlwqdzJHBhZ2luZz1UcnVlwqdzJG9uZ2xldD3Cp3MkZnJlZXNjb3BlPUZhbHNlwqdzJHdvSVM9RmFsc2XCp3Mkd29TUENIPUZhbHNlwqdzJGZsb3dNb2RlPUZhbHNlwqdzJGJxPcKncyRzZWFyY2hMYWJlbD3Cp3Mkc2VhcmNoQ2xhc3M9&scrll=DZ%2FREFERENCE%2FCONTRATS-NUMERIQUE%2F2020%2FPARA%2F221.21

Pierre Esplugas-Labatut, « Derrière le respect de la dignité de la personne humaine, le retour du gouvernement des juges ? », *AJDA*, https://www-dalloz-fr.lama.univ-amu.fr/documentation/Document?ed=etudiants&ctxt=0_YSR0MD1tZXRvb8KneCRzZj1zaW1wbGUtc2VhcmNo&ctxtl=0_cyRwYWdlTnVtPTHCp3MkdHJpZGF0ZT1GYWxzZcKncyRzb3J0PSNkZWZhdWx0X0Rlc2PCp3Mkc2xOYlBhZz0yMMKncyRpc2Fibz1UcnVlwqdzJHBhZ2luZz1UcnVlwqdzJG9uZ2xldD3Cp3MkZnJlZXNjb3BlPUZhbHNlwqdzJHdvSVM9RmFsc2XCp3Mkd29TUENIPUZhbHNlwqdzJGZsb3dNb2RlPUZhbHNlwqdzJGJxPcKncyRzZWFyY2hMYWJlbD3Cp3Mkc2VhcmNoQ2xhc3M9wqdzJHRhYlJmdD03M0Q1QTkzQg%3D%3D&id=AJDA%2FCHRON%2F2022%2F0355

Thomas Cassuto, « Droit et intelligence artificielle », 2018, https://www.dalloz-actualite.fr/chronique/droit-et-intelligence-artificielle

Décisions de justice

Arrêt n° 650 du 9 déc. 2019, 18-86.767

Arrêt de la CJUE du 20 décembre 2017, affaire C434/16, Nowak

Cass., ass. plén., 10 nov. 2017, no 17-82.028 , JCP 2017. 1376, obs. C. Ribeyre ; JCP déc. 2017, no 52, p. 1366, obs. A. Gallois ; Procédures janv. 2018, no 1, comm. 23, obs. Chavent-Leclère ; D. 2018. 103, note Décima ; AJ pénal 2018. 100, obs. Kurek
Crim. 13 oct. 2004, no 00-86.726 , Bull. crim. no 243

Cons. const. 8 juill. 1989, n° 89-258 DC et Cons. const. 2 mars 2018, n° 2017-693 QPC

Décision Conseil constitutionnel n° 2021-817 DC 20 mai 2021

V. Paris, 8 févr. 1995, aff. Schuller/Maréchal, D. 1995. 221, note Pradel. – Puis arrêt de rejet : Crim. 27 févr. 1996, no 95-81.366, D. 1996. 346, note Guéry ; JCP 1996. II. 22629, note Rassat

Table des matières